Bottlenecks & challenges and RTD responses for legal, social, ethical, and economic aspects of healthgrids : V3.0

DOBREV, A.; STROETMANN, V.; STROETMANN, K.; VAN DOOSSELAERE, C.; WILSON, P.; Andoulsi, Isabelle; Herveg, Jean

Publication date:
2007

Document Version
Publisher's PDF, also known as Version of record

SHARE

BOTTLENECKS & CHALLENGES AND RTD RESPONSES FOR LEGAL, ETHICAL, SOCIAL, AND ECONOMIC ASPECTS OF HEALTHGRIDS – ROADMAP I

Document ID:	**SHARE-D4.1-revised_v3.0.doc**
Date:	**06/07/07**
Authors:	**I. Andoulsi, A. Dobrev, J. Herveg, V. Stroetmann, K. Stroetmann, C. Van Doosselaere, P. Wilson**
Activity:	**WP4: Ethical, Legal and Socio-Economic Aspects of healthgrids – Baseline**
Document status:	**V3.0**
Document link:	**http://eu-share.org/deliverables.html**
Confidentiality:	**Public**
Keywords:	**healthgrid, Legal, Ethical, Social, Economic, Bottlenecks & Challenges**

Abstract: This document describes the baseline of European level legislation that might have an impact on the implementation and exploitation of grid technology in the healthcare setting and introduces ethical considerations of the use of technology in the healthcare setting. The deliverable also provides a baseline of economic analyses tools that are useful in assessing the potential impact of the adoption of such technologies.

Document Log

Issue	Date	Comment	Author
0	14/09/2006	Economic analysis contribution	V. Stroetmann
1	20/9/2006	Confidentiality contribution	I. Andoulsi
1.1	3/11/2006	Confidentiality editing	P. Wilson
1.1	12/11/2006	Confidentiality comment	C. Van Doosselaere
1.2	16/11/2006	Liability Issues Contribution	I. Andoulsi
1.3	10/12/2206	Liability Issues Edit	P. Wilson
1.4	19/12/2006	IPR issues contribution	I. Andoulsi
1.5	07/01/2007	IPR edit	P. Wilson
1.6	02/02/2007	Final Edit and Comment	P. Wilson
1.7	08/02/2007	Additional contributions	V. Stroetmann, A. Dobrev
1.8	09/02/2007	Revisions and initial quality review	K. Stroetmann
1.9	10/02/2007	Quality review of overall document	S. Robinson
1.10	10/02/2007	Additional contribution Final edit and Comment of the legal part	I. Andoulsi
1.11	11/02/2007	Final Edit and release	P. Wilson
2.0	12/02/2007	Final Release	Y. Legré

2.1	02/05/2007	Revision of introduction Addition of legal references	I. Andoulsi
2.2	21/05/2007	Editing	C. Van Doosselaere
2.3	21/06/2007	Integration of introduction on ethics (from P. Wilson's work on D4.2)	C. Van Doosselaere
3.0	04/07/07	Final version	N. Jacq

Table of Contents

1. GENERAL INTRODUCTION ON THE LEGAL, ETHICAL AND SOCIO-ECONOMIC BASELINE

The health and social services sector is an important, even a dominant economic sector in the European Union. In 2000, the sector employed more than 15 million people – more than 9% of European employment – making it a more important employment sector than retail with 13.0m workers or business services with 13.3m workers. The gross *value added* of the health and social services sector amounted to almost 500 billion euro – more than 6% of European Union GDP –, topped only by business services with 513.7 bn euro.[1] Looking only at the *human* health sub sector, for which more detailed and comprehensive data are available, total health *expenditure* accounted for 8% of GDP in the EU-15 in 2000. On a per-capita basis, health expenditures in current US$[2] varied from high values of 2,514 for Luxembourg and 2,422 for Germany to only 884 in Greece and 862 in Portugal. Furthermore, health is in itself a wealth factor for a nation, those who are healthy can work and contribute to the economy. In the words of David Byrne when he was European Commissioner for Health:

> *"Modern economies are built on good health. Their competitiveness increasingly depends on enabling their citizens to lead healthier, more productive lives. Good health is a key driver of growth. There is evidence that a 10% rise in life expectancy can generate up to 0.35% in GDP increase. Put simply, health generates wealth. Each health euro better spent could make a net saving both for individual well-being and for EU competitiveness. This is why achieving good health must become an economic priority."*[3]

[1] These are only rough figures due to considerable differences in national statistics on which these data are based.

[2] Data available only in US$ from the World Bank (from Jan. to Dec. of 2000, the exchange rate changed from about 1 USD for 1 € to about 1 US$ for 1.06 €).

[3] Press Release IP/04/934, Boosting the economy through better health: Commissioner Byrne launches reflection process on the future of EU health policy, Date: 15/07/2004

However, although the figures quoted above are impressive, we should recall they are European averages, and hide significant variation across the 27 Member States. With the expansion of the European Union by ten new Member States in 2004 and two new accessions in 2007 as well as a further three Candidate Countries still in waiting, significant disparities between three separate country groups become apparent. Whereas three of the new Member States Cyprus (888), Malta (807) and Slovenia (788) almost reach the expenditure per capita level of Greece and Portugal, the latest two New Members Romania (48) and Bulgaria (59) fall far below even the low mean value (218) for all of these 12 countries, and reach only about 3% of the mean value (1,818) for the old Member States.

It should also be noted that despite its significant role within the European economy, the healthcare sector is quite different from almost any other economic sector: it is highly regulated with often little competition, being mostly characterised by public sector actors financed from public or quasi-public sources such as taxes or public health insurance funds. There is strong pressure to reduce costs and improve economic efficiency in the health sector. Healthcare expenditure is expected to continue to rise, yet the already high expenditure levels measured as percentage of GDP, quoted above, indicate that the scope for further increase is limited. The scope for increase in demand for more, better, safer, and timelier healthcare, on the other hand, is unlimited. As a consequence, a key challenge that healthcare systems are facing is optimising the use of resources in order to meet this increasing demand within a context of budgetary constraints.

In order to address some of these differences and challenges the European Union has used its funds, including its various

framework programmes for RTD, to support the development of ICT applications in the health sector, much in the same way as national funds have targeted the use of ICTs to improve health services access, delivery and safety. The overriding goal of all these activities has been to contribute towards better health and care across Member States, in particular through implementation and diffusion of eHealth products and services including support for regional, national and trans-European eHealth infrastructures. It is expected that this will contribute to better medical outcomes, better quality of life for citizens and patients, more efficiency, and improved access. However, the results of the programmes have been mixed at both EU[4] and national[5] level and they have only recently gained in scope and relevance for healthcare professionals and citizens.

If it is accepted therefore that the healthcare sector is of economic importance, and that for the main it operates within the regulated framework of the public sector, it is very important that regional, national and supranational policies to advance the development and implementation of ICT for health are based on a solid understanding of the economic and regulatory aspects of adopting the new technologies and applications. Accordingly in this deliverable we provide a baseline of key legal, regulatory and economic issues that need to be taken into account by policy makers in seeking to support a wide adoption of Grid Technology in the healthcare sector.

Set against this background we can see that the adoption of emerging technologies like Healthgrid to best effect, when this

[4] Cf. Veli N. Stroetmann, Karl A. Stroetmann with Stefan Lilischkis, edited by Data-Bank Consulting: IST Impact Study: Microelectronics & Microsystems, Health, Mobile Communications - Health Domain -: Study for the European Commission, Bonn/Milano/Brussels, November 2004: ftp://ftp.cordis.lu/pub/ist/docs/about/final_report_part_b_health.pdf

[5] For details, see Stroetmann KA, Stroetmann VN: Electronic business in the health and social services sector - Key issues, case studies, conclusions. Sector Impact Study No. 10-II. The European e-Business Market W@tch, Brussels/Bonn, August 2004, available at http://www.ebusiness-watch.org.

may mean changing established and valued working and clinical practices, will also face significant organisational and medico-cultural challenges.

However, the use ICTs in healthcare is a reality. ICTs applications are used daily in surgical planning, clinical decision support and radiological examination, to name just a few examples. Information technology also forms the backbone of hospital administration and is beginning to play a significant role in community care administration as well. Most patients are now happy to recognise that their healthcare records are stored electronically and, to varying degrees, shared within and across healthcare institutions so that physicians and carers have access to up-to-date and validated patient information where and when they need it. Advances in research promise also that in the near future more and more citizens will be ready to make use of and even demand remote monitoring and assessment technologies to allow them to receive healthcare support at home, work and play without having to use the traditional hospital and primary care services.

According to an earlier study, eHealth ICTs such as healthgrids are emerging as the new industry, alongside pharmaceuticals and the medical devices sector, to become the third largest industry in the European health sector. The study suggested, for example, that by 2010 spending on eHealth technology may account for up to 5% of the total health budget of the 25 Member States from just 1% in 2000 for 15 Member States[6]. Although the enormous double-digit growth would imply are not being realised at present, European industry has every opportunity to become a leading global player in this growing industry if a wider, more integrated European market can be established, supporting their *competitive* position in a growing

[6] SIBIS, Benchmarking Highlights 2002: Towards the Information Society in Europe and the US, May 2003. See http://www.sibis.org/.

global health ICT market[7]. This, in turn, will support *sustainable growth* and the creation of *new and better jobs.*

For this reason, it is important that well constructed roadmaps for new eHealth technologies are adopted so that necessary steps can be taken along the way to ensure not only that research and technological development will create new tools, but that the legal and regulatory framework is ready to accommodate them. Similarly, the economic realities into which the new tools are designed to fit must be carefully studied in order to ensure that a maximum number of business case arguments can be made to show the potential contribution to both health and wealth of using new technologies such as healthgrids. Finally, the organisational realities and dynamics, including change management and training/education issues, need also to be considered for a successful deployment and diffusion. Similarly, the legal and regulatory issues must be addressed because one of the key challenges of the organising the health sector arises from the fact that one of the core components of any healthcare transaction – patient data – is very complex.

[7] See Deloitte and Touche (2003) eHealth: HINE - Health Information Network Europe; 2003 report. Considering present constraints on spending in this market, this is probably a by far too optimistic estimate. On the other hand, Frost & Sullivan estimates in its 2004 report on The Market for Telemedicine in Europe that just this segment will grow till 2010 to about $ 1.8 bn or around 42% per annum, an even more optimistic - and in all likelihood totally wrong - prognosis.

2. LEGAL AND REGULATORY ASPECTS OF HEALTHGRIDS

2.1. INTRODUCTION

In any healthcare setting the amount of personal health data collected is voluminous, difficult to collect, and changes over time. As medical technology has advanced, the process 'components' that make up the full continuum of care have increased in number and sophistication. This presents healthcare providers with a continuously increasing amount of data and information to work with. It is only logical to favour information management, sharing and re-use of data as the primary purpose of implementing ICT solutions. It is rational to expect that not only old models of healthcare will be enhanced by the introduction of ICT into the processes, but also that ICT will facilitate, even necessitate the creation of completely new models of healthcare. Grid technologies are a primary example of emerging ICT that facilitates a new model of healthcare and in particular of health-related research.

However, patient information and healthcare data in general are protected by the legal and ethical duties of confidentiality to which all healthcare providers are bound. If therefore the European healthcare systems are to be made more accessible, safe and sustainable at least in part through the implementation of ICTs within healthcare workflow and processes, then we must carefully study the extent to which the legal regulation of handling and processing of medical data are adapted to the use of such ICTs.

A common factor among eHealth tools is that they store, process, forward and share data. Some of that data is administrative, some related to objects, such as in radio-frequency identification based tracking of devices, but a great deal of the data is the personal data of patients. Healthcare professionals know they have a duty of confidentiality and a duty of care -they want to exercise both fully in order to provide a safe environment in which patients are treated with due

respect for their privacy. The duty to provide care is undoubtedly served by sharing patient records, providing on-line support to colleagues and even giving direct support to patients in their homes via the internet… but how does it sit with the co-existing duty of confidentiality?

In Europe the approach has been, on the whole, less technical and focused instead on traditional human rights values of privacy. As a result of the European Data Protection Directive, the Member States of the European Union have generally adopted legislation that focuses primarily on the individual's right to privacy and secondarily on the need of medical professionals to share healthcare data.
The purpose of this report is to explore the nature of the **European level** response to medical privacy through a detailed examination of the data protection directive as well as other relevant legislation.

However, data privacy is not the only legal issue that should be addressed in road mapping healthgrids. It is also vitally important to assess the extent to which product and services liability is adapted to meeting the challenges of healthgrids, as well as considering the wider legal-economic issues such as intellectual property rights.

The three clusters of legal issues addressed in this report were developed during WP4's initial work with WP3 on D3.1, where the technology baseline was drawn. Based on the various milestones or phases set in the technology baseline, and on the subsequent work on bottlenecks and roadblocks, it was felt that these clusters of issues would most likely create an obstacle to

the further development of the technology at its various phases were data protection, liability and intellectual property.

This report will accordingly look in detail at the EU level legislation that covers:

A. Confidentiality and Data Protection
B. Product and Services Liability
C. Intellectual Property Rights

For each of these three issues, a "Questions and Answers" session has been drawn to ensure reader-friendliness from as wide an audience as possible. Using the Questions and Answers form should render these complex issues more discernible and understandable to a non-expert audience, thus facilitating reactions and comments from a wide community and enabling WP4 to take into account the user needs and requirements in the next documents to be produced.

2.2. CONFIDENTIALITY AND DATA PROTECTION

2.2.1.Introduction

The key principles relevant to the processing of personal data were first established by the Council of Europe,[8] and further developed in Directive 95/46/CE of the European Union – the European Data Protection Directive.[9] The latter is the major source of legislation, although the Recommendation made by the Council of Europe is also of importance for the healthcare sector and for the use of grid technology in that sector, since it focuses on the field of medical data and scientific research.

The Directive provides a general framework for the protection of privacy with respect to the processing of personal data in its widest sense. It is important to note here that the Directive is

[8] Convention No. 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data adopted on 28 January 1997; Recommendation No. R (97) 18 of Committee of Ministers to Member States concerning the protection of personal data collected and processed for statistical purposes, adopted on 30 September 1997.

[9] Directive 95/46/CE of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and free movement of such data, *OJ L 281*, of 23 November 1995, 31-50.

based on the privacy of processing of data, not privacy *per se*. Thus, the Directive does not confer any special rights of privacy of an individual which might be covered in a Member State's constitution, but rather it provides rules about how personal data may be processed so that the processing itself does not infringe the privacy of an individual. Within the terms of the Directive a suitable level of privacy is to be afforded to all data related to a natural person, whether the context of such information is the private, public or professional life of the individual. The Directive thus goes beyond the concept of private life and intimate detail.

The primary purpose of the Directive is to allow the free flow of personal data between the Member States of the European Union, in order to facilitate the establishment and the functioning of the internal market, while its secondary purpose is to protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of their personal data. The protection granted by the Directive does, however, go further than the protection of the natural person's intimacy, i.e. generally speaking the protection of each natural person private life. It applies more particularly to any sensitive data relating to natural persons such as data concerning health -including mental health.

2.2.2. To what data does the data protection directive apply?

In deciding if the Directive applies to a particular set of data one must therefore first ask if the data allow the identification of a particular natural person and second if the data are going to be processed by someone (a legal or natural person). The basic principle here is that if a piece of information (a laboratory result) can be linked to a person either by reasonably simple means or even by or with the help of a third party, then the data are considered as identifiable and therefore in the scope of the Directive. It should be noted that this concept is usually construed quite widely. Thus, if the information refers to a group or if it is so complete or so unique as to make it

applicable to only a very small number of people (e.g., disease profile, age, gender, postcode, profession all held together) then the data could be classified as identifiable even if no actual identifier is used.

Given the wide construction it is easy to see that the data contained in a healthgrid, even if not identified by a patient's or a study subject's name, will be covered by the terms of article 2(a) of the Directive which states that the term '**personal data**' relates to; *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".*

2.2.3.To whom does the data protection directive apply?

The data protection rules are addressed primarily to the **data controller**, i.e., the legal name of the person who decides the purpose and the means of the processing. This person has the legal duty to ensure that data are handled appropriately in order to ensure the right level of privacy. The data controller is usually a senior staff and who is officially named as the data controller by organisation's governing body. Although the controller is always a natural (real) person, he does not necessarily have to belong to a formally constituted body.

2.2.4.What are the main duties of a data controller?

Any personal data that the controller needs to process for the purposes of his professional or other activity must meet a certain level of quality. This means that the controller must comply with the Directive's principles concerning data collection and data processing.

First, this means the **data may only be collected for specified, explicit and legitimate purpose.** In practice that will require the controller to define clearly and precisely the

purpose(s) for which the data are to be processed. The controller will therefore have to notify the relevant national authority that he is intending to collect personal data and must set out clearly what data will be collected and for what reason. The controller should also be able to explain the purpose and process of the data collection and handling to the data subject.

Second, the **purpose of the processing must be legitimate**. The Directive lists the general conditions under which the processing will be presumed as legitimate and the national legislation further defines what types of data processing are legitimate.

We noted earlier that the overarching purpose of the Directive is to protect privacy within the context of the growth of the internal market. This means that to be legitimate the interests in the data processing must outweigh the interests of the data subject in excluding the processing of the data. Medical data processing is usually legitimate processing because the data subject will have a significant interest in her health data being shared with appropriate professionals if the sharing of the health information will allow better and safer healthcare delivery.

Generally a controller may only process personal data for the purpose that was given when the data were first collected. In some cases, the controller may want to re-use the data for another purpose. This will only be legal if the secondary use falls under the uses covered by the national legislation. In many Member States such re-use is permitted if it is for statistical, scientific or historical purposes.

Furthermore, the **data collected should be adequate** for the stated purpose but not excessive. If a researcher collects data in order to carry out a specified research project, he may not collect other data that are not necessary for the study in hand

but might be useful at some later date. Once the data are collected, the controller must keep them up-to-date for as long as they are needed for the specified purpose, but should not keep them longer than necessary, and must render them anonymous or destroy them when the pre-defined purpose of processing has been achieved.

If the data are to be processed by a third party – a **data processor** – this means in practice that the contract between the data controller and the data processor must include a clause that the data processor shall act only on instruction of the data controller and that he is also legally responsible in case of any breach of data confidentiality.

The controller also has a duty to ensure that data are stored and processed securely by taking appropriate technical and organisational measures to ensure the security and confidentiality of person identifiable data**.** According to Article 17 of the Directive, the controller has the obligation to ensure the security of the personal data processed, meaning that he must ensure that the data are not lost, altered, or accidentally destroyed. In order to achieve those two purposes, the controller must implement appropriate technical and organisational measures to protect personal data against, for instance, accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.[10] In other words, the controller has to construct his system to render it sufficiently secure for the processing of personal data.

This might also imply that in a healthcare setting a structural reorganisation of the hospital or research institute is undertaken to ensure the confidentiality and the security of the data processed. This might include the appointment of a data protection officer in charge of the data protection issues. On the other hand, technical measures could include restricted access

[10] Directive 95/46/CE, art. 17, 1, § 1.

to the databases to authorised persons and the utilisation of software protecting the system against viruses or hacking.

Processing **nominative or identifiable** data in medical research grid would be legitimate if research were given as the purpose of the processing at the time of collection. However, the controller of a healthgrid must ensure that **nominative or identifiable** data are not kept for longer than necessary for the originally defined purpose -in a longitudinal of multi-purpose research study it will therefore usually be necessary to keep the data in an anonymous or pseudonymous form. Furthermore where **nominative or identifiable** data are stored reasonable steps must be taken to hide the true identity of a data subject. Given that the nature of grids is to share the data – often over national boundaries – the steps taken to protect the data must be commensurate with the processing technology. In other words, because a grid is a hi-tech application, state of the art security technology must be used to protect that data stored and processed in the grid.

2.2.5. Are all personal data treated in the same way by the Directive?

A general principle provides that the level of protection offered by the Directive to personal data depends not on the information content, but on the purpose of the data processing. In other words, the potential or actual infringement for the fundamental rights and freedoms of the data subject of privacy and autonomy will be assessed on the basis of the purpose of the processing of personal data.

However, a key indicator remains in the nature of the data. Some data are considered as sensitive and in need of special protection. This is the case of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, as well as data concerning health or sex life and judicial data. For these data the protection depends on the content of the information *and* on the purpose

of the data processing. Therefore article 8 of the Directive prohibits the processing of medical and other sensitive data.

The ban, however, is not absolute. The Directive sets out a number of cases in which the collection and processing of medical data may be legitimate. As a result the national legislation of the Member States will allow processing of medical data if:

- The controller has obtained the explicit informed consent of the data subject; *or*
- If the data are collected to protect the vital interest of the data subject or of another person when the data subject is physically or legally incapable of giving his consent; *or*
- The data are collected for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services *and* if the data are processed by a health professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

The Directive provides the possibility for the Member States to add exemptions for reasons of substantial public interest that could be subject to further specific safeguards, such as the authorisation of the national supervisory authority. Thus, a national transposition of the Directive might allow for the adoption of a national exemption for scientific research or for social security reason.

According to the exemptions to article 8, as listed in its paragraphs and sub paragraphs, a healthgrid containing **nominative or identifiable health data** will be legal in terms of data protection only if the **explicit consent** of the data subject was obtained before the data were collected. If this did not happen then the data in the grid are handled by a medical doctor AND the purpose of the grid is

the further preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services. If the person handling the data is not a medical doctor but a research scientist he or she will have to be contractually bound in his or her employment contract to maintain the confidentiality of the data. **The only case in which these criteria need not be met is where the Member State in question has passed specific legislation which provides different terms for data collection and processing for the purposes of medical, scientific or historical research.**

2.2.6. What rights does the Directive give to the data subject?

The general purpose of the Directive is to facilitate sharing of data in the context of the internal market while allowing the data subject to retain appropriate control over the data. Accordingly the Directive requires that data subjects have access to information about the type of data held and the purpose for which it is processed and further the data subject must be allowed to have any errors in the data rectified or, under some conditions, to object to the processing and have it stopped.

A distinction is made between cases where the data are collected directly from the data subject and where they are collected indirectly. If the data are collected directly from the data subject the controller must provide at least identity (name, address, denomination or trade name, etc.) and a description of the purposes of the processing. These purposes have to be specified and explicit, which means that a precise description of the scientific or the statistical project must be given. The processing of sensitive data or medical data normally requires the provision of further information. Guidelines provide, for example, that in case of genetic analysis, the data subject should be informed about the objectives of the analysis and about the possibility of unexpected findings.[11]

[11] See Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the protection of medical data adopted on 13 February 1997.

When personal data have not been obtained directly from the data subject, the controller should, before considering the way of processing these personal data or the right time to inform the data subject, assess whether they comply with the requirements for re-use of data.[12]

Moreover, the duty of information does not apply when data are indirectly collected for processing for statistical purposes or for the purposes of historical or scientific research, if the provision of such information is impossible or would involve a disproportionate effort.

All data subjects have the right to request specific information about their own personal data that are processed by the controller. Moreover, where medical data are processed, data subjects may ask a healthcare professional to exercise their access right. Upon request, the controller will then have to provide the data subjects with information such as whether or not data processing of data relating to them is taking place. He will also have to inform them about the purpose of the processing, the categories of data and the data being processed, the recipients or categories of recipients to whom the data are disclosed and the source of the data. However, the Directive allows Member States to exempt the controller from respecting the data subject's access right where the purpose of the processing is scientific research, or when data are kept in personal form for a period which does not exceed the period necessary to create statistics. The Directive, however, subjects the granting of that exemption to the condition that there is clearly no risk of breach of the data subject's privacy. Moreover,

[12] See paragraph 2.2. supra.

data may not be used in order to take measures or decisions regarding any particular individual.

Under the Directive, a data subject has the right to ask for data to be corrected, erased or blocked where their processing does not comply with the provisions of the Directive.[13] This is particularly the case where personal data are incomplete or inaccurate. This right means that the controller must correct, erase or block the data as required by the data subject, in a reasonable period. Blocked data cannot further be processed, used, or communicated without the data subject's consent. In addition, if the controller has disclosed the data to third parties, he has to notify them about any correction, erasure or blocking carried out. This notification of correction, erasure or blocking of data does not have to be performed if it proves to be impossible or involves a disproportionate effort.[14]

The Directive allows Member States to exempt the controller from the obligation to respect the data subject's right of correction in case of processing for purposes of scientific research, or when data are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.[15] Furthermore the Directive provides that the data subject has the right to object to the processing of his data. When there is a legitimate objection to the data processing, the controller may no longer process the concerned data or communicate them to recipients, and must ensure they are erased.[16]

The controller of a healthgrid must therefore first ensure that he knows from whom the data is being collected, because if it is being collected directly from a data subject he must inform the data subject about the purpose of the collection. This may be implicit information if

[13] Directive 95/46/CE, art. 12(b).

[14] Directive 95/46/CE, art. 12 (c).

[15] Directive 95/46/CE, art. 13, 2.

[16] Further to this the Council of Europe has recommended in Recommendation No. R (83) 10 on the protection of personal data used for scientific research and statistics, that where processing is conducted for scientific or statistical reasons, the data subject may withdraw his collaboration. This is however not binding upon Member States, but is considered as good research practice.

the controller is the data subject's treating doctor, but in the case of a scientist collecting data for research purposed directly from the data subject the purpose should be explicitly stated. If the data are being drawn from existing records the data subject should be informed about the research if it is not unduly difficult or costly to do so. Next he must ensure that he can grant access to the data subject to his data if he requests it, unless national legislation provides that this is not necessary. If any of the provisions safeguarding the data subject's interests are not complied with, the data subject would have the right to demand that his data are withdrawn from a study or database. It is therefore very much in the scientist's interests to ensure he complies with the legislation because not only might national legislation levy a fine for non-compliance but also a data subject could severely disrupt a study if he discovered that data were unlawfully held and decided to exercise his right to have them erased. The scientist should also ensure that the data collected are accurate, because if they are not the data subject has a right to demand they be corrected and, if this is not possible, that they be erased.

2.2.7. What are the implications for Cross-Border Data Sharing?

Healthgrids provide doctors, researchers and health system planners the opportunity to support areas of healthcare such as medical imaging and image processing; modelling the human body for therapy planning; pharmaceutical research and development; epidemiological studies; and genomic research and treatment development. However, in order to be truly effective such grid applications must draw together huge amounts of data from disparately located computers – which of course implies data sharing across jurisdictions and the sharing of responsibilities by a range of different data controllers.

National legislations of the different EU Member States are now for the most part harmonised, and the transfers of personal data between these Member States should not create a problem. Thus, a data controller of a healthgrid established on the territory of one Member

State can, in theory, be sure that in transferring the data he processed to another controller established in another Member State, that these data would be correctly protected as the second Member State provides for the same level of protection of personal data as his own.

This would be the case if all Member States had transposed the Directive in the same way. But differences are already to be found in the Member States' legislations as regards the definitions of key concepts of the Directive such as 'personal data', 'processing' or 'controller'. Moreover, the Directive itself allows the Member States to *"adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:*

(a) national security;

(b) defence;

(c) public security;

[…]".

There might thus be differences in the level of protection granted to personal data between the EU Member States, which might be a problem for the implementation of the healthgrid technology on the whole territory of the European Union. However, it is important to note that even if there are differences in the levels of protection of personal data between the Member States, these differences are of minor importance, as the implementation of the Directive already ensures a high level of protection for personal data. These differences in the levels of protection of personal data between the Member States cannot even constitute barriers to data transfers as Article 1, paragraph 2 of the Directive prescribes:

"Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1 (i.e. the protection of data subjects' fundamental rights and freedoms)".

This is not always the case as regards the transfer of personal data towards other countries located outside the European Union and the European Economic Area (EEA), where data protection is governed by specific conditions[17] that need to be met in addition to the requirements for the communication of personal data to third parties as analysed above. If the destination country is not in the European Union, the general rule is that the controller should refrain from transferring personal data to a recipient located in non-EEA countries. However, the Directive provides that if the data subject gives his consent unambiguously to the proposed transfer or if the transfer is necessary for the performance of a contract between the data subject and the controller (as might be the case for healthcare) or if the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party (as might be the case in medical research undertaken for a specific patient or group of patients) or if the transfer is necessary in order to protect the vital interests of the data subject, such a transfer can take place towards countries located outside the European Union and the EEA.

Moreover, the Directive states that Member States may authorise a transfer or a set of transfers of personal data to a third country that does not ensure an adequate level of protection of personal data, where the controller adduces adequate safeguards through appropriate contractual clauses between the sender and the recipient of the personal data. In this context, the European Commission proposes standard contractual clauses that ensure an adequate level of protection of transferred personal data.

However, the European Directive does not set specific conditions for the transfer of **medical** data to non-EU (and non-EEA) countries, but the Recommendation No. R

[17] Directive 95/46/CE, articles 25 and 26.

(97) 5 of the Committee of Ministers to Member States on the protection of medical data, adopted on 13 February 1997, does. It establishes additional rules for the transfer of medical data to a country that does not have an equivalent level of protection of medical data as the one granted on the territory of the European Union.

Furthermore, some countries, such as Argentina, Isle of Man, Guernsey and Switzerland, have been recognised by the European Commission as ensuring an adequate level of protection. This means that the European Commission has decided that these countries have a level of protection of personal data in some way equivalent to the one available in the Member States of the European Union. The transfer of data to companies or other legal entities located on the territory of the United States that adhere to the US Department of Commerce's Safe Harbour Privacy Principles is also allowed. The European Commission moreover allows the transfer of personal data to recipients located on the territory of Canada, provided that these recipients are subject to the Canadian Personal Information Protection and Electronic Documents Act (also called the 'PIPED Act').

2.2.8. Are there special rules for processing and sharing genetic data?

The European Directive does not contain all the rules relating to the processing of medical or genetic data. Some specific rules relating to the processing of medical data have been proposed by the Council of Europe within Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the protection of medical data, adopted on 13 February 1997. It should be noted that these are guidelines and not legally binding.

The Recommendation provides that only healthcare professionals or individuals or bodies working on behalf of those healthcare professionals should carry out the processing of medical data. Those individuals or bodies should be subject to confidentiality rules equivalent to those incumbent on healthcare professionals.[18] Moreover medical data must normally be obtained directly from the data subject, but it is possible to obtain such data from other sources of information when some conditions are met (as provided for in the Directive). Finally, medical data should not be communicated to third parties unless some conditions are met. As regards the processing of genetic data, the Recommendation No. R (97) 5 establishes that genetic data that are collected and processed for preventive treatment, diagnosis or treatment of the data subject or for scientific research, should only be used for those purposes.

Many healthgrid initiatives will be established to process and share genetic data. It should be noted that for these data no specific rules exist at EU legal level and that therefore the normal rules described above will apply. However, the Council of Europe's Recommendation No. R (97) 5 provides guidelines that state that genetic data that are collected and processed for preventive treatment, diagnosis or treatment of the data subject or for scientific research, should only be used for those purposes. So, a healthgrid controller using genetic data should, as a matter of good practice, be aware of the recommendations and should be able to comply with them.

[18] This requirement is equivalent to the one contained in Article 8, 3 of the European Directive which provides that *'Paragraph 1 shall not apply where processing of data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy*".

It is also important to underline that other specific rules exist for the processing of other person-identifying data, when the purpose of the processing is scientific or statistical. Recommendation No. R (83) 10 of the Committee of Ministers to Member States on the protection of personal data used for scientific research and statistics, adopted on 23 September 1983, proposes different principles for the processing of these data for research or statistics purposes. It recommends that, where possible, research should be undertaken with anonymous data; only if using anonymous data renders the research impossible, should person identifiable data be used.

2.2.9. Are there any legal rules concerning network security?

The discussion above on the Data Protection Directive has clarified that the data subject has rights, including a right to access the data. The networks hosting data processing therefore have to be suitably adapted to be able to ensure that the data are kept secure and that, where appropriate, they can be corrected.

The confidentiality and security requirements for data processing, whether in a Grid or any other computer architecture, are mainly regulated in the 8th section of Directive 95/46/EC.

Article 16 of the Directive provides that *"any person acting under the authority of the controller or of the processor including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law"*. The controller must therefore ensure the confidentiality of the personal data,

meaning that unauthorised access to them or disclosure must be prevented.

Article 17 of the Directive governs the security of the processing, according to which the controller has the obligation to ensure the security of the personal data processed, meaning that he must ensure that the data are not lost, altered, or accidentally destroyed.

In order to meet the obligations of articles 16 and 17 the controller must implement appropriate technical and organisational measures to protect personal data against, for instance, accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.[19] In other words, the controller has to construct his system to render it sufficiently secure for the processing of personal data. He should also ensure that the organisational structure of his company is adequate to ensure the confidentiality and the security of the data processed.[20]

This means that the protection of the data enclosed in the system has an impact on the system itself. The data controller must collaborate with the network controller to fulfil the confidentiality and security requirements. The infrastructure must be confidential to protect the rights of the patients. It must also be secure and stable enough to prevent any damage to the data collected, processed and stored. According to the law,[21] the appropriate level of protection to ensure depends of the state of the art, the cost of the system's implementation, the risks represented by the processing, and the nature of the data

[19] Directive 95/46/CE, art. 17, 1, § 1.

[20] An example of an organisational measure could be the appointment of a data protection officer in charge of the data protection issues. On the other hand, technical measures could include restricted access to the databases to authorised persons and the utilisation of software protecting the system against viruses or hacking.

[21] Directive 95/46/CE, art. 17, 1, § 2.

to be protected (for instance sensitive data, like health data require a higher level of protection).

In a healthgrid, a number of data controllers and data processors will work together. In such circumstances, the data controllers must reinforce security and confidentiality measures because the information collected are disseminated to another person who will process it. Each original data controller (i.e., the original collection point) should then ensure that the processors provide sufficient guarantees on technical security measures and on organisational measures governing the processing to be carried out and on the fact that he will comply with those measures. The European Directive requires that in such cases the processing should be governed by a contract or by a legal act binding the processor to the controller and stipulating in particular that the processor shall only act on the instructions of the controller and that he should be responsible for taking all appropriate technical and organisational measures.

2.2.10.Conclusion

The discussion of the basic concepts and duties of the Data Protection Directive and its impact on healthgrids shows that when healthgrids are used for treating patients or planning care the requirements of the legislation provide that so long as the data subject has consented or the data are collected and processed by medical professionals the balance of rights weighs in favour of data collection -that is, it is assumed that the patient's general interest in obtaining treatment or advancing medical care outweighs his interests in privacy.

However, most of the newly developed health grid applications that exist and are currently running are for longer term purposes – that is, research, preventative medicine or healthcare planning – and are not controlled by medical professionals but rather by research scientists. Where this is the case, Member States have the possibility to enact specific legislation covering specific tools such as healthgrids in order to exempt the scientist using running healthgrids from some of

the more onerous duties of the Directive. Member States could, for example adopt specific legislation to encourage the linking of diagnosis specific databases across a region or state in order to support research into a given disease. However, no Member States has specifically addressed legislation to this particular issue and so healthgrids drawing the data and data processing power of many hospitals together are burdened with heavy data protection requirements which could deter scientists from adopting healthgrid technology and using its enhanced computational and data acquisition power.

Perhaps more significantly little attention has been paid to the specific needs of data sharing for healthgrids across European borders and outside the Union. If healthgrids are really to grow to their full potential and deliver their promises, adjustments must be made to national and supranational legislations to re-assure would-be healthgrid users that it is legal to share health related data using grid technology. This in turn implies the development and adoption of robust guidelines developed specifically for the healthgrid context which address the balancing of interests between an individual's privacy and medical advancement.

2.3. PRODUCT AND SERVICES LIABILITY

2.3.1.Introduction

As we saw in the first part of this analysis, implementing a healthgrid generally implies the processing of patients' health

personal data, which in turn implies risks for patients' rights and liberties. Implementing a healthgrid and using it in a hospital for instance, implies other risks for patients. Indeed in case of malfunctioning of the system or of problem in the supply of services, patients could be harmed. It is possible that a malfunctioning healthgrid could cause a wrong decision to be made and thus injury or harm to be caused to patients. Yet at present, there is no specific European legislation covering such eventualities. In order to understand the legal liabilities of a healthgrid controller as they are provided for at a European level we have to look at general product and services liability legislation.

In the health sector legal aspects of medical liability are most commonly regulated at the health provider-patient level. Thus when a patient is the victim of medical negligence or of a medical error, the legal questions are usually solved on a simple basis of professional liability. In general, this is an issue solved through national law, based in most European Countries in a **no-fault liability** rule in torts – that is, if a patient is harmed, he is compensated regardless of the intent of the healthcare practitioner. This is not, however the case in all EU Member States. In some cases, there may of course be allegations of criminal negligence or even criminal intent, in which case the healthcare professional might face prosecution.

However, not all doctor-patient relationships are simple. In fact, for most medical treatments delivered in hospital or specialist

care settings, a number of healthcare practitioners will be involved in the care of the patient: clinical specialists, nurses, radiologists, radiographers etc. Determining the responsibilities for each one has become difficult. Who should be regarded as liable in the event of problems? The doctor? All the members of the medical team in charge of the patient? The hospital?

In the case of a medical establishment operating a healthgrid and perhaps making diagnostic decisions based on the information provided in the Grid, the problems become even more complex. Even if at first the medical liability has to be considered in the relationship between the patient and the healthcare practitioner,[22] the establishment of the person to be held responsible for a specific damage can be problematic when taking into account the number of intermediaries participating to a healthgrid and the complexity of such a system involving different actors such as doctors, specialists, hospitals, pharmaceutical companies, data controllers and processors, technicians, etc., often located in different countries.[23]

As noted above there are no specific liability rules applicable to products and services possibly supplied by the healthgrid systems or composing them. Such interaction will therefore be assessed, in terms of legal liability, on a general principle that products and services provided to consumers must comply with a certain level of quality.[24]

[22] The principle is that a patient victim of a medical negligence or error will at first bring proceedings against his doctor. The generalist is thus the front line in case of medical damages caused to a patient.

[23] As stated by senior researcher Jean Herveg in the report *Legally e-Health: Product Liability and Consumer Protection* (to be published), in the healthcare practice, the patient is nowadays frequently aware of the different intermediaries in charge of his file. In case of damage, he could then logically bring proceedings against them rather than against his doctor. Difficulties could then occur from the differences in the way their responsibility is been engaged. On the other hand, the patient is more and more in charge of his health, without the intervention of a healthcare practitioner. Thus, beyond the articulation of the different healthcare practitioners' liability, there are situations where the patient is no more taken in charge by a healthcare practitioner. Under these circumstances, the patient stands alone against the pharmaceutical companies or the medical devices companies which might be subject of different rules regulating their liability. It might thus be impossible for the patient to find an interlocutor and to obtain compensation for the damage caused to him.

[24] This principle applies mutatis mutandis to business-to-business relations. See infra.

At a European level, a range of legislation has been adopted in order to protect consumers. They provide, in general, consumers with a legal guarantee of high level quality products and services. They also contain provisions dedicated to the redress of damages resulting from sub-standard products and services.

Even if these texts are not directly dedicated to products and to services that are supplied by healthgrid systems or that compose them, they can be easily applied there. In this section we will therefore first consider the European legislation applicable to the information contained in the healthgrid systems or to the products and the services supplied by these systems. We will then look at the legal texts to determine the responsibilities of the different actors of healthgrids, in particular as regards the elements that compose these systems. Finally, we shall outline some general eHealth situations, such as pharmaceutical products sold via Internet and contracts concluded electrically, in which the particular responsibility of certain actors of the system is determined.

2.3.2. Who bears responsibility for the security of data in a healthgrid?

As stated in the first part of this document, processing of personal data requires security and confidentiality of information highways. These requirements encompass both levels of the information system. To ensure the confidentiality and the security of the data processing performed in the framework of the second level of the information system, the infrastructure (which constitutes the first level of the information system) must be secure and stable.

In terms of confidentiality, any person acting under the authority of the data controller or of the data processor, including the data processor himself, who has

access to personal data, must not process them except on instructions from the controller.[25]

In a healthgrid the data controller in due cooperation with the network controller must implement appropriate technical and organisational measures to protect personal data. There are thus three important actors: the **data controller**, the **data processor** and the **network controller**, who have to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, etc.

If a healthgrid is not maintained securely and the data in it can become corrupted and in turn give rise to incorrect and/or misleading data outputs which could result in harm to a patient, the data controller would then be liable in case of damage caused to a patient and he would be responsible to compensate for the damage. Article 23 of the Data Protection Directive provides that *"Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered".*

However, the data controller would have a defence if he could prove that he is not responsible for the event giving rise to the damage. He could, for example, prove that a default of maintenance of the system by the network controller gave rise to the patient's damage.

2.3.3. Do website hosts have a legal liability for what happens on the site?

While most healthgrids at present are not used to providing content for health related websites targeted at the general public, it is conceivable that in the not-too-distant future grid technology could be used to provide real-time feeds to publicly accessible databases of information on, say, a current outbreak of influenza. In this

[25] Directive 95/46/EC, art. 16.

type of scenario a website would automatically be populated with data to advise travellers on vaccination needs. The question might therefore arise as to who would be liable if the website showed an incorrect body of data and a citizen were harmed?

The "eCommerce" Directive 2000/31 on certain legal aspects of information society services provides some answers in that it provides for special rules to minimise the risks for technical partners of eHealth services providers, who act as 'intermediaries'. For instance, in principle, a company that provides server space for website hosting to an ePharmacy will not be liable for the illegal sale of medical products or for the damage caused by wrong information delivered to patients. The Directive establishes a special exoneration system of liability for some categories of Internet intermediaries providing information society services called 'Mere Conduit', 'Caching' and 'Hosting' under specific circumstances.

Mere Conduit: "Mere Conduit" consists in the transmission in a communication network of information provided by a recipient of the service or the provision of access to a communication network. A mere conduit service provider is not liable for the information transmitted as long as the provider does not initiate the transmission nor select, nor modify the information contained in the transmission.

Caching: A caching service provider is not liable for the automatic, intermediate and temporary storage of the 'cached' information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request. A caching service provider must not modify the information stored. He must comply with conditions on access to the information, with rules regarding the updating of the information. He must not interfere with the lawful use of technology to obtain data on the use of the information; and must act quickly to remove or to disable access to the information stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or

access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

Hosting: When providing a "Hosting" service, the service provider is not liable for the information stored at the request of a recipient of the service. The hosting provider must not however have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent. If he becomes aware of such activity he must act quickly to disable access to the information.

2.3.4. Who is responsible if a faulty product is delivered through a healthgrid?

Although a healthgrid itself will not deliver a product, it might be the direct link to the delivery of a product in that a product might be delivered through healthgrid systems to patients, such as medicinal products, pharmaceutical products or any other kind of products used in relation with the patient's health. Indeed, this is already the case at a London hospital where an ePharmacy has been set up through a combination of ePrescribing, eDispensing using a robot system, eStockmanagement and eProcurement, for outpatients and discharged patients. Similarly, one can imagine a grid in which formulas can also be provided to different biomedical experts using a healthgrid.

The question arises therefore as to who would be liable if damage occurs as a result of a faulty product delivery? At present we have no clear legal answers, but would instead have to apply the general principles of consumer protection.

These principles dictate that if a product does not conform to the offer made or causes damages, the consumer (or another person representing him) may claim for

compensation. Any liability issue will thus normally depend on the general rules of law applicable in the different EU Member States.

2.3.5. What is the EU doing to protect citizens in this context of vague legal duties and responsibilities?

The European legislation around product and services liability can be distinguished into two broad types: 1. those concerned with the prevention for harm and 2. those that allow recourse for damage or an unsatisfactory product. In the healthgrid domain it will be mainly the former that applies – that is, the **General Directive on Product Safety** (Directive 2001/95 of the European Parliament and of the Council of 3 December 2001 on general product safety).

2.3.6. Why is Directive 2001/95 on general product safety relevant to healthgrids?

The Directive on General Product Safety imposes a general safety requirement to products placed on the market and intended for consumers or likely to be used by them. The Directive is designed to ensure that producers put on the market only products that are not likely to cause any threat (or only a reduced threat in accordance with the nature of the product's use) and that allow the effective protection of consumers' health and safety. In addition, they must provide consumers with relevant information to enable them to assess the risks inherent to the product, particularly when these risks are not obvious. They *must* also take appropriate actions to avoid these risks (withdrawal of unsafe products from the market, warning of the consumers, recall of unsafe products already supplied, etc.).

In order to understand the impact this legislation will have on healthgrids, we must first establish what sort of products it applies to – and define 'product'. In the framework of Directive

2001/95, the term '**product**' means any product which is intended for consumers or likely, under reasonably foreseeable conditions, to be used by consumers even if not intended for them, and which is supplied or made available, whether for consideration or not, in the course of a commercial activity, and whether new, used or reconditioned. Therefore, products initially reserved for professional use that are subsequently made available to consumers are also covered by the Directive's definition of the term product.

The Directive applies only to goods and products on the market for consumers to acquire, whether for free or for consideration. Since most healthgrids applications are not yet designed or foreseen for the general market, the Directive has only limited application for now. However, once that changes, the Directive will become relevant to suppliers of Grid component software – some of which may have a health application. We can already see the use of grid computing in consumer areas such as digital content sharing and application service provisioning, it is surely only a matter of time before some of those applications are also in the health arena.

2.3.7. How does the General Product Safety Directive work in practice?

Member States have established or designated national authorities to monitor product safety and to take appropriate measures as regards risky products. Every national authority must ensure that producers and distributors comply with their duties and are entitled to ensure product safety by organising checks on safety properties, by imposing producers to warn adequately on the possible risks, by prohibiting dangerous products to be marketed, by alerting consumers on the risks of a product already marketed and by organising recalls and destruction of products when necessary.

Any producer or distributor who discovers that a product is dangerous must notify the competent national authority and collaborate with it to ensure that all relevant consumers are made aware of the risks.

Directive 2001/95 also aims to create an efficient information system in order to help EU Member States, national authorities and consumers to react quickly in order to avoid or to reduce any harm caused to persons' health and safety.

2.3.8.And what if something goes wrong anyway?

When a defective product causes damages, rules contained in Directive 83/374/EEC on Liability for Defective Products will apply.[26] This Directive aims at ensuring a high level of consumer protection against damage to health or property by a defective product. It also aims to reduce the disparities between national liability laws that distort competition and restrict the free movement of goods. Finally, it implements a system that extends the producer's liability (called the 'strict liability') in order to protect consumers.

When the producer, importer or supplier, is considered as liable, he must pay compensation for the damage caused to the person or to his properties, but only for that resulting from a defect. Though, in order to strike a reasonable balance between the interest of the consumer and the need to encourage innovation and technological development, the Directive contains some rules protecting the producer. Also, the injured person has a limited period of three years to seek compensation. This period starts from the day on which the claimant became aware, or should reasonably have become aware of the damage, the defect and the identity of the producer. After that, no further compensation will be possible. In any case the producer's liability is limited to a period of ten years from the date on which the producer puts the product into circulation. This time limit is intended to preserve a balance between consumers' and producers' interests.

[26] Council Directive 85/374 of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, *O.J. L210,* 7 August 1985, p. 29-33.

Directive 85/374 Liability for Defective Products establishes the principle of objective liability (or liability without fault) of the producer, importer and in some circumstances the supplier of a defective product. The producer, importer or supplier, will be liable and must pay compensation for damages caused to persons or properties but only for that resulting from a defect. The claimant person does not have to prove that the producer was at fault or negligent; he simply needs to prove the damage, a defect and a direct causal relationship between defect and damage.

2.3.9. Does any other law protect a consumer in a healthgrid?

One of the important goals of the healthgrid systems used in the healthcare sector will be to deliver medicinal products or medical devices to patients. The patients can thus acquire products necessary for the preservation of their health by means of the system. Therefore in the eHealth arena, when the product delivered does not conform to what was foreseen in the contract, citizens can have recourse to the relevant national legislation based on the Directive 1999/44/EC on Sale of Consumer Goods. [27]

According to the **Directive on Sale of Consumer Goods** when consumer goods are sold under a contract, the seller must deliver goods in conformity with the sale contract. Moreover, when a commercial guarantee exists, the seller or the producer will be legally bound to that guarantee as well as to the associated advertising. The commercial guarantee will have to be made available in writing (or another durable medium, such as an e-mail) and will have to contain some information. Anyone selling an eHealth product would have to comply with these rules, and conversely a purchaser of an eHealth product would have redress under them.

[27] Directive 1999/44 of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantee, *O.J. L171,* 7 July 1999, p. 12-16.

In the framework of Directive 1999/44, the definition of the **consumer** is the same as the one of Directive 1997/7 on the protection of consumers in respect of distance contracts.[28] The consumer is thus described as any natural person who, in the contracts covered by the Directive, is acting for purposes that are not related to his trade, business or profession. **Consumer goods** covered by the Directive are any tangible movable item (except goods sold by authority of law, water and gas where they are not put up for sale in a limited volume or set quantity, and electricity).

The **seller** is any natural or legal person who, under a contract, sells consumer goods in the course of his trade, business or profession, when the **producer** is defined as the manufacturer of consumer goods, the importer of consumer goods into the territory of the Community or any person purporting to be a producer by placing his name, trademark or other distinctive sign on the consumer goods.

2.3.10. So what does the Directive on Sale of Consumer Goods mean to ordinary people?

The seller has to deliver to consumers goods that are in conformity with the contract of sale.

Consumer goods are presumed to be in conformity with the contract if they:

(a) comply with the description given by the seller and possess the qualities of the goods which the seller has held out to the consumer as a sample or model;

(b) are fit for the purposes for which goods of the same type are normally used;

(c) are fit for any particular purpose for which the consumer requires them and which he made known

[28] Directive 1997/7 on the protection of consumers in respect of distance contracts, *O.J. L144,* 4 June 1997, p. 19-27.

to the seller at the time of conclusion of the contract and which the seller has accepted;

(d) show the quality and performance which are normal in goods of the same type and which the consumer can reasonably expect, given the nature of the goods and taking into account any public statements on the specific characteristics of the goods made about them by the seller, the producer or his representative, particularly in advertising or on labelling.

The seller is not liable if, at the time the contract was concluded, the consumer was aware, or could not reasonably be unaware of, the lack of conformity, or if the lack of conformity has its origin in materials supplied by the consumer.

2.3.11. But healthgrid systems are not only about data and products!

Services might also be delivered through healthgrids, such as virtual courses in real time for undergraduate graduate students, young professionals in the case of medical eLearning or for matters such as second opinions, demonstrations, or medical assistance of tourists or expatriates.

Equally simulations and modelling for therapy planning and computer-assisted interventions and large multi-centre epidemiological studies are typical clinical services that might be delivered through healthgrids.

So what is the responsibility of the professionals concerned in the supply of these services? As mentioned above, services available through healthgrid applications

are diverse. They might be passive services, such as supplies of general medical information through networks or Internet workstations for end-users. They might also be active services like medical advice or specific decision support to clinicians, or might involve the collection of biomedical data for remote monitoring by clinicians.

Such services might conceivably cause damages to those who depend on it. A citizen might for instance follow bad advice and fall ill, be harmed or even die. A clinician might follow the recommended procedure after using a decision support tool and might consequently harm his patient.

However, it must be noted that at present there is no **European** harmonisation of liability rules for the delivery of services. Liability in case of problems in the supply of services through healthgrid systems will therefore be governed by **ordinary rules of law applicable in the different EU Member States, which might not be satisfactory.**

2.3.12. And what if a healthgrid forms part of a medical device?

When a product considered as a medical device is placed on the market, specific additional rules regarding the safety of those particular products apply. Directive 93/42/EC concerning medical devices[29] aims notably to safeguard patients' and users' health and safety by harmonising the conditions for placing medical devices on the market and putting them into service. Among other conditions, medical devices must be designed and

[29] Council Directive 93/42 of 14 June 1993 concerning medical devices, *O.J. L169*, 12 July 1993, p. 1-43.

manufactured in such a way that their use does not compromise the safety and health of patients, users and other persons when properly installed, maintained and used in accordance with their intended purpose.

Moreover EU Member States are involved in the protection of patients. Indeed, when one of them notes that a medical device conforming to the Directive's prescriptions compromises the health and/or safety of patients, users or, where applicable, other persons, it shall take all appropriate interim measures to withdraw it from the market, prohibit or restrict it being placed on the market or put into service.

2.3.13.So what is a Medical Device?

According to the Directive's text, a '**medical device**' is:

> " […] any instrument, apparatus, appliance, material or other article, whether used alone or in combination, including the software necessary for its proper application intended by the manufacturer to be used for human beings for the purpose of:
>
> - diagnosis, prevention, monitoring, treatment or alleviation of disease,
> - diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap,
> - investigation, replacement or modification of the anatomy or of a physiological process,
> - control of conception,
>
> and which does not achieve its principal intended action in or on the human body by pharmacological,

immunological or metabolic means, but which may be assisted in its function by such means".

The accessories that are not medical devices as such, but that are specifically intended to be used together with a device to enable it to be used as wanted by the manufacturer, shall be treated as medical devices.

For vendors and users of healthgrid systems it is important to note that electronic equipment and software must be regarded as within the definition of medical device, when they are manufactured or promoted for medical purpose.

According to the Guidelines Relating to the Medical Devices Directive[30] available on the website of DG Enterprise,[31] software related to the functioning of medical devices are medical devices on their own if placed on the market separately from the related devices. When software helps to emit a diagnosis (like image enhancing software created for diagnostic purposes), or is a therapeutic tool, it has to be considered as a medical device. This is not the case for software used for the administration of general patient data.

The manufacturer's obligations set out in the Directive, must also be fulfilled by the natural or legal person who assembles, packages, processes, fully refurbishes and/or labels one or more ready-made products and/or assigns to them their intended purpose as a device. This subparagraph does not apply to the person who, while not being a manufacturer within the meaning

[30] These guidelines aim at promoting a common approach by manufacturers and Notified Bodies involved in the conformity assessment procedures according to the relevant annexes of the Directive and by the Competent Authorities charged with safeguarding Public Health. Nevertheless, they are not legally binding. However, due to the participation of the aforementioned interested parties and of experts from Competent Authorities, it is anticipated that they will be followed within the Member States and, therefore, ensure uniform application of relevant Directive provisions.

[31] For details and references see *http://ec.europa.eu/enterprise/medical_devices/meddev/index.htm*.

of the first subparagraph, assembles or adapts devices already on the market to their intended purpose for an individual patient.

In the Directive's context, manufacturers are obliged to place on the market or to put into service only medical devices that do not compromise the safety and health of patients, users and, where applicable, other persons, when properly installed, maintained and used in accordance with their intended purpose. The manufacturer must design and manufacture medical devices in such a way that some 'essential requirements' are met, such as to take into account the generally acknowledged state of the art and to eliminate or reduce risks as much as possible (like the risks linked to the toxicity of certain materials and their incompatibility with biological tissues and cells, or the risks of contamination for persons involved in the transport, storage and use of medical devices).

Devices that are in accordance with the national provisions transposing the existing European harmonised standards will be presumed by EU Member States as compliant with the essential requirements laid down by the Directive. Devices other than those which are custom-made or intended for clinical investigation must bear a CE conformity mark when placed on the market.

2.3.14. What about the electrical equipment that forms part of the components of a healthgrid?

When the products manufactured are electrical or constitute electronic equipment, like IT or telecommunications equipments, they shall respect the provisions of the RHoS Directive, which relates to restrictions of the use of certain hazardous substances in electrical and electronic equipment. This Directive imposes manufacturers to avoid using lead, mercury, cadmium, hexavalent chromium,

polybrominated biphenyls (PBB) or polybrominated diphenyl ethers (PBDE) in those equipments.

However, the Directive does not currently apply to medical devices, even if the definition contained in the Directive's text could cover electronic equipments and software. Furthermore, the possibility of applying the RoHS Directive to the manufacturers of hardware products is debated. A possible interpretation of the Directive would be that hardware sold to medical equipment manufacturers in order to run medical equipments, but which retain all functions of a computer, will have to respect its prescriptions. Nevertheless computers or other compounds installed into medical equipments that do not act as separate tools, but only operate the medical device, are to be considered as medical devices and are not concerned by RoHS Directive.

2.3.15. What about the liability in more general issues such as Internet based health information provision and sale of health related goods over Internet?

Although healthgrids are at present not used much for giving the general public access to health information or for selling goods, it is worth looking briefly at these issues.

In terms of liability the key point is that, from the moment a service is proposed by Internet at the individual request of a recipient of services normally provided for remuneration, it is considered as an **information society service** and rules of the Directive on eCommerce (2000/31/EC) are to be respected. Thus, if a doctor or a pharmacist is running a health related website, this means that they will have to inform the website users of their identity, address, VAT number, etc. This **information duty** aims to enable the recipient of the service (professional or not) to identify properly the service provider and to ensure transparency of his activities.

The purpose of the information duty is to allow the ultimate users to know against whom they can seek recourse if they should need to do so.

If a health related website includes commercial communications (i.e. any type of communications promoting goods, services or the image of a company), the Directive on electronic commerce imposes additional duties on services providers. It requires, among other things, that the person on whose behalf the commercial communication is made be clearly identifiable and that commercial communication be clearly identifiable as such as well. The purpose of this rule is to avoid any confusion between **advertising** and any other type of information.

2.3.16.Liability in Contract

So far we have looked at the EU level Directives and Guidelines that regulate liability for goods and services provision, and we have noted that most of it is applicable to healthgrids by analogy only. Thus, were a healthgrid forms part of a medical device, the special liability rules for medical devices will have to be followed, or where a patient suffers damage as a result of a decision taken based on a healthgrid the doctor who is sued by the patient may have recourse against the supplier of the healthgrid.

However, most eHealth business will necessarily involve the conclusion of contracts. These contracts contain the description of the various parties' obligations and, often, special clauses. When one of the parties does not respect his obligation, the contract will thus constitute a helpful tool to determine the liabilities. Under these circumstances, general national contract law will apply, transposing where applicable European legislation.

If the contract for delivery of the eHealth product or service happens online, as may well be the case, then the Directive 1997/7 on Distance Contracting[32] as well as some rules of the Directive on Electronic Commerce will apply. The Directive on distance contracts applies only to contracts concluded between professionals and consumers, while the Directive on electronic commerce applies to business-to-consumer transactions and to business-to-business transactions, except when the professional parties are allowed to agree otherwise.

The key points to note are that the Directive on **distance contracts** (1997/7/EC) imposes on the supplier a duty to provide the recipient with written information (including e-mail or online information) about his identity, the product or the service and its price, prior to the conclusion of the contract, and must allow the recipient a cooling off period of 7 days which begins on the day the product is received.

In the context of contracting it should be noted that **electronic signatures** are, according to EU legislation, to be treated as equal to hand written signatures. Different kinds of electronic signatures exist, from the very simple ones (the insertion of a scanned hand-written signature within an electronic document), to the most sophisticated ones, such as the signatures based on public key cryptography. This last kind of signatures implies the intervention of a trusted third party in order to allow the recipient to check the identity of the sender and the integrity of the message.

[32] Directive 97/7 on the protection of consumers in respect of distance contracts, *O.J. L144*, 4 June 1997, p. 19-27.

Directive 1999/93/EC on electronic signature provides the conditions for the legal recognition of any electronic signature and provides that where the signature is based on a public key cryptography system (**advanced electronic signature**), it benefits a more favourable regime. When the conditions are met, the advanced electronic signature is considered as having the same effect as a hand-written signature. In case of problems with a prescription or with a diagnosis, it will be easy to determine the author of the mistake. However, even simple eSignatures such as scanned signatures can have legal value: if a doctor uses his scanned signature for a medical order in a legal proceeding the judge cannot *a priori* refuse to consider this type of signature but must analyse, with possibly the help of experts, the evidence value of this signature. The advantage of the use of advanced electronic signature is that, in the context of a trial, this type of signature is directly considered as having the same evidence value as the hand-written signature.

2.3.17.Conclusion

We have seen that determining the responsibilities of each actor within the framework of healthgrid systems is not easy. While the rules on Data Protection are reasonably well adapted to the eHealth domain generally, the same cannot be said for the liability rules which will apply to a wide range of actors and which will need to be determined legally in the event that a patient suffers harm as a result of a decision taken on the basis of information shared through a healthgrid.

Accordingly it is important the existing European framework of general product safety is re-examined to consider its applicability to distributed networks such as healthgrids.

Furthermore the law on medical devices is very unclear with respect to healthgrids. While it may be argued that a healthgrid could fall within the ambit of the current Medical Devices Directive in that it is a software tool that impacts on a medical act, the whole construction of the Directive is based upon physical goods (which might have a software component) that are placed on the market for purchase or lease, it is ill adapted to deal with the shared domain of grid-based services where software sold and owned by a wide range of participants.

It would seem therefore that at present the only real way to have clarity over liability for the possible negative effects of healthgrids is through tightly constructed contracts in private law. If however the use of healthgrids across EU and international borders in shared public/private initiatives is to become a reality then steps should be taken to develop guidelines and possibly legislation to harmonise the legal expectation of all actors in a healthgrid.

2.4. INTELLECTUAL PROPERTY RIGHTS

2.4.1.Introduction

The healthgrid vision relies on the setting up of grid infrastructures for medical research, healthcare and life sciences. This implies the availability of data organised in databases. This also implies the availability of grid services, most notably for data and knowledge management.[33]

A fully functioning healthgrid will be composed of a **data grid**, i.e. a distributed and optimised storage of large amounts of

[33] These services must be deployed on infrastructures involving healthcare centres (e.g. hospitals), medical research laboratories and public health administrations. For details on this point see, SOLOMONIDES, T., *"Structuring and supporting healthgrids Activities and Research in Europe (SHARE): towards a European healthgrid, step one"*, e-Science 2006, Amsterdam, 4-7 December 2006.

accessible information and of a **computing grid** which implies the utilisation of numerous computers, computer programmes and other electrical components. The final part of a full healthgrid would be a **knowledge grid** or in other words, the intelligent use of a data grid for knowledge creation. This knowledge grid has not yet been deployed. As we say repeatedly in this document, a healthgrid is thus mainly composed of computers and computer programs and encompasses databases.

As the implementation of healthgrids on the territory of the European Union grows, so will the protection of databases assume an increased importance, given that most grid services will be provided via electronic databases accessible online, offline or accessible via European-wide networks. Databases should therefore be accorded an appropriate level of protection so as to create an attractive environment for investments while safeguarding users' interests.

As researchers Laura Vilches Armesto and Philippe Laurent noted, medical data is usually addressed by lawyers from a privacy point of view. As they go on to say,

> *"However intellectual property is increasingly put forward when discussing the control, the use or the transmission of medical data. Even if medical data relates to patients and is moreover protected by very strict data protection and secrecy rules, this information is nonetheless "created", sorted, structured, explained and, more generally, processed by professional practitioners and medical administrations. Given this processing of the data and drafting of files and reports concerning health condition of patients, one could indeed assume that these intellectual investments should be worth some legal protection".*[34]

[34] Laura VILCHES ARMESTO and Philippe LAURENT, « Intellectual property on medical data - chimaeras and actuality », *Acts of the 16th World Congress on Medical Law*, Toulouse, 7-11 August 2006, p. 747-754.

This is not the case only for medical data: adequate legal protection is also required for molecular data, cellular data, tissue data and even population data.

We will therefore look in some detail at the EU level legislation that seeks to protect intellectual property in databases as well as certain aspects of the law of copyright.

2.4.2. What does Directive 96/9/EC on the legal protection of databases mean for healthgrids?

The Directive on the legal protection of databases, which was adopted in February 1996, can apply to databases constituted of medical, genetic or even general data, as regards its definition of a database. The Directive creates a legal framework of rules for the protection of a wide variety of databases in the information age by giving a high level of copyright protection to "original" databases[35] and a new form of *"sui generis"* protection to those databases which were not "original" in the sense of the author's own intellectual creation (those databases are also called "non-original" databases). In other words the Directive introduced a new specific *sui generis* right for the creators of databases, whether or not these have an intrinsically innovative nature.

The Directive defines a **database** as *"a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means"(art1(2)).*It thus applies to databases in any form, but does not apply to the software used in the making or operation of the database or to the works and materials contained therein. Nor does it affect the legal provisions covering patents, marks, designs and models or unfair competition that can apply to the database or to its contents. Given this wide definition, the Directive can apply to much of the contents of a healthgrid.

[35] See infra for a definition of this concept.

2.4.3. What sort of database can be copyrighted?

First, it must be remembered that the granting of copyright does not require any specific legal procedure. Any literary or artistic works, which includes amongst others, any production in the scientific domain[36], so long as the works are expressed in a certain form and are original, can be copyright material. Copyright will therefore usually apply to the structure of databases, but rarely to the content (unless that is totally original too). To gain copyright, a database must have originality in the selection or arrangement of the contents and may be regarded as an intellectual creation particular to its author. Each individual item included in the database may or may not be in copyright, depending on its originality.

A database of electronic health records could then be capable of being copyrighted, given that the healthcare practitioner has completed the records in an elaborate and original way. This could also be the case for genetic[37] or tissue databases.

[36] Definition proposed in « Intellectual property on medical data - chimaeras and actuality », *opcit,* p. 747.

[37] For a detailed analysis of copyright protection for genetic databases in the United States see, Ray K. HARRIS and Susan Stone ROSENFIELD, "Copyright Protection for Genetic Databases", *45 Jurimetrics,* 2005, p. 225-250.

Copyright protection could apply to the database comprised of tissue samples once the tissue data were coordinated and arranged in an original structure that could for instance help researchers.

2.4.4. What rights does Copyright give the creator of a database?

The creator or the author of the database enjoys a group of exclusive rights to carry out or to authorise:

(a) temporary or permanent reproduction by any means and in any form, in whole or in part;

(b) translation, adaptation, arrangement and any other alteration;

(c) any form of distribution to the public of the database or of copies thereof. The first sale in the Community of a copy of the database by the right holder or with his consent shall exhaust the right to control resale of that copy within the Community;

(d) any communication, display or performance to the public;

(e) any reproduction, distribution, communication, display or performance to the public of the results of the acts referred to in (b).[38]

However, a legitimate user of a database may perform all the acts referred to in article 5 of the Directive that are necessary for using the database.

However, the protection granted to databases by Directive 96/9/EC might seem insignificant compared to the efforts and the energy demonstrated by data grid creators in order to retrieve in each case, molecular, cellular, tissue or personal data. Only the structure of these databases is protected, while value for sure still resides in the samples of the databases for development of enhancements, competing technologies or follow-on products.

[38] Directive 96/9/EC on the legal protection of databases, art. 5.

2.4.5. But what about protecting the data content of the healthgrid?

Directive 96/9/EC introduced another protection for databases besides copyright. It created a new exclusive *sui generis* right for database producers. *Sui generis* rights protect the substantial investment of the database producer from a quantitative and qualitative perspective, in the obtaining, verification or presentation of the contents of the database.[39] There is thus a new EU level protection granted for the investment made (financial and in terms of human resources, effort and energy) in the obtaining, verification or presentation of the contents of a database.

So, in terms of protection granted, the difference between the structure, the content and the investment made for the development of a database is very important. Traditional **copyright** protects the structure of databases, while ***sui***

[39] Directive 96/9/EC on the legal protection of databases, art. 7(1). See also recitals 40 to 42 of the Directive.

generis rights protect the investment made for the development of databases.

In the framework of *sui generis* protection, the producer or the maker of a database (i.e. the person who made the investment), whether a natural or a legal person, can prohibit the unauthorised retrieval and/or re-use of its contents.[40] Protection against unauthorised retrieval or re-use is accorded to databases whose maker is a national, a company or an undertaking resident in or having his/its registered office, central administration or principal place of business in the Community.

2.4.6. Does that mean no one can use the content of a healthgrid database without consent?

No, the Directive states that *"non-substantial extractions and reuses may be undertaken by third parties, without the right owner's authorisation, as long as these acts are not made in a repeated and systematic way that would imply a conflict with the normal exploitation of the database or produce an unreasonable prejudice to the legitimate interests of the database's maker".*[41]

The fact that non-substantial parts of a database may be extracted and re-used in another database might cause a prejudice to other interests than the ones of the database maker. For instance, the extraction of information from a database containing medical records might cause a prejudice to patients' rights. There can thus be a contradiction between this right to re-use non-substantial parts of a database to create another database for example and the legislation applicable to

[40] Directive 96/9/EC on the legal protection of databases, art. 7(1). The terms extraction and re-utilisation are defined in article 7(2) of the Directive. In this framework, extraction shall be seen as the permanent or temporary transfer of all or of a substantial part of the contents of a database to another medium by any means or in any other form. On the other hand, re-utilisation shall mean any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission. The first sale of a copy of a database within the Community by the right holder or with his consent shall exhaust the right to control resale of that copy within the Community.

[41] Directive 96/9 on the legal protection of databases, art. 7(5), a contrario.

the protection of the data which requires for any re-use of data relative to a patient, the agreement of the patient.

Furthermore, the right to prevent even substantial extraction and re-use of the contents of a database extends for a period of 15 years with effect from the date on which the database was terminated.[42]

A further point to note is that during the 15 year period, *sui generis* rights are pecuniary rights and as such can be transferred, assigned or granted under contractual licence[43]. Again, this is of importance when the data are personal medical data.

The combination of these two principles, i.e. the economic nature of the *sui generis* rights and their term of protection for a period of 15 years, may constitute an impediment for the deployment of healthgrids. Database makers could for example charge third parties wanting to develop data grids before granting them their *sui generis* rights under contractual

[42] Directive 96/9 on the legal protection of databases, art. 10(1). In the case of a database which is made available to the public in whatever manner before expiry of the period provided for in paragraph 1 of article 10, the term of protection by that right shall expire fifteen years from the first January of the year following the date when the database was first made available to the public. Finally any substantial change, evaluated qualitatively or quantitatively, to the contents of a database, including any substantial change resulting from the accumulation of successive additions, deletions or alterations, which would result in the database being considered to be a substantial new investment, evaluated qualitatively or quantitatively, shall qualify the database resulting from that investment for its own term of protection (art. 10(3)).

[43] Directive 96/9 on the legal protection of databases, art. 7(3).

licence. There might thus be an impediment in terms of costs to the implementation of healthgrids. On the other hand, in the pharmaceutical sector, researchers might claim *sui generis* rights on certain databases. Such claims could delay the release of other products which could have been discovered on the basis of the information contained in the first database compiled in another way.

Given these constraints it should not be surprising that businesses in the Member States have not welcomed the Directive with open arms. Indeed an evaluation conducted on the basis of a 2005 online survey addressed to the European database industry and of the Gale Directory of Databases (the "GDD") showed that the *sui generis* right seem to have caused considerable legal uncertainty. DG Internal Market and Services invited stakeholders to comment on four options: repeal the whole directive (option 1); withdraw the *sui generis* right while leaving protection for creative databases unchanged (option 2); amend the *sui generis* provisions in order to clarify their scope (option 3); maintain the status quo (option 4). Although a significant number of responses were received the Commission found the results inconclusive and have invited further comments from stakeholders on economic repercussions of this

type of protection. At the time we publish this document (winter 2006-spring 2007), that consultation is still open.

2.4.7. What does the Copyright legislation mean for patients' data?

A database author has the right to control the reproduction and the communication of his work to the public. However, it is not certain how that right balances against the rights of patients whose data is held within the database. Some authors have argued that when a database is constituted of electronic health records, cellular or tissues, the work is *"[…] created with data relating to patient(s), (their) bodies, (their) health and the treatment they undergo. These data (are) subject to very strict sensitive data protection and privacy rules"*.[44] Thus the patient's rights and the protection of sensitive data are superior to the copyright which would have a direct impact on the exercise of authors' exclusive rights. For instance, an author could not prohibit to the patient the access to and the use of a copy of his medical record. The author or copyright owner could thus no longer exercise their exclusive rights alone. This could impede the development of databases and as a consequence the development of healthgrids.

One of the possible solutions would be to introduce a distinction between various types of data, as the medical data and the health data or sanitary data. In the case of electronic health records, it would be advisable among others to determine the status of the personal notes of the doctor. Indeed, most of the blockings seem to come from the absence of clear and precise definition of the notion of medical datum.[45]

2.4.8. What about Intellectual Property Rights and Biobanks?

[44] « Intellectual property on medical data - chimaeras and actuality », *opcit,* p. 748.

[45] Philippe VANLANGENDONCK, « Le dossier médical électronique : problèmes de vie privée et de responsabilité », sur *http://www.droit-technologie.org*, p. 1-10. For developments on this topic see the Roadmap document.

As already mentioned in this document, a **database** is a collection of independent elements, including artistic, literary, musical works, texts, data or other materials arranged in a systematic way and individually accessible by electronic or other means.[46]

It contains a wide range of items that may be protected by copyright – as explained above – and by other intellectual property rights such as patents.

This is especially the case for **biobanks**, i.e. for databases containing biological materials. Biobanks are mainly used in the drug discovery sector, by pharmaceutical companies, research laboratories, universities or hospitals, in order to 'test drive' medicinal products to be put on the market. In the field of drug discovery, various actors with different interests collaborate to the development of future medicinal products. The different intellectual property rights applicable to biobanks render the situation even more complicated for those actors.

Biobanks are to be considered as databases. The fact that they contain biological material does not lead to their exclusion from

[46] Recital 17 and article 1, paragraph 2 of Directive 96/9/EC on the legal protection of databases.

the database regime. Biobanks are thus to be seen as composed of structures and contents.

As already explained in this document, copyright protects the structure, as long as it is original. The way different biological materials are sorted, classified, linked together and rendered accessible through menus or entries, may thus be copyrighted.

But in this context, **contracts** will play a key role in order to determine who will be the copyright owner of a particular database. Indeed, depending on the terms of the contracts pertaining to the creation of the structure of the biobank, and their role in that creation either the practitioner, the hospital or any other contractor such as a pharmaceutical company or any combination of them could be the copyright owner. In some cases, this could help a research laboratory or a pharmaceutical company to prevent that the medicine it discovered be copied

by a competitor. In that context, however, it is important to underline that some third parties such as universities or academic research laboratories might benefit from certain exceptions to the ban to copy or to communicate the database's structure to the public, in specific circumstances such as the use of the database for teaching or scientific research purposes.

Biobanks may also be protected by *sui generis* rights. The owner of those rights will then be the hospital or the research laboratory that has made the investment in order to constitute the database. The *sui generis* rights owner will then be allowed to prohibit the substantial extractions and re-use of the database by any third party. In the drug discovery sector, this could also be of importance for pharmaceutical companies or research laboratories developing medicinal products. The *sui generis* rights will help them protect their discoveries by

preventing any competitor to copy their biobanks in order to develop similar products.

However it is important to note, as researchers Laura Vilches Armesto and Philippe Laurent do[47], that the *sui generis* rights protection is weaker than copyright because only biobanks demanding a substantial investment for their constitution may be protected.

Furthermore, in application of Directive 1996/9/EC, *"non-substantial extractions and re-uses of a database may be undertaken by third parties, without the right owner's authorisation, as long as these acts are not made in a repeated and systematic way that would imply a conflict with the normal exploitation of the database or produce an unreasonable prejudice to the legitimate interests of the database's maker".*[48]

[47] « Intellectual property on medical data - chimaeras and actuality », *opcit,* p. 752.
[48] Directive 96/9 on the legal protection of databases, art. 7(5), a contrario.

Finally, according to the *spin-off* theory[49] a biobank that would result from activities whose main purposes are not the creation of a database for drug discovery for example, could not benefit from the *sui generis* rights protection.

Last but not least, the content of biobanks, i.e. the biological materials contained in biobanks could also be patented. Indeed, the research carried out and the developments made on the basis of biobanks' contents could result in inventions, more specifically in biotechnological inventions.

At European level, these inventions are protected by Directive 98/44/EC.[50] This directive is at the source of a potential opposition between the rights of the patients and the right to patent an invention, similar to that between the rights of the patients and the copyright materials. Indeed Recital 26 of the Directive provides that the patient who has given biological material that has served as the basis of an invention in the frame of a biobank, must give his free and informed consent as regards the filling of a patent application on such invention, according to his national legislation.

The fact that this measure is part of the Directive's introduction, what makes it an ethical rule rather than an applicable provision, and the fact that several Member States did find it controversial and too advanced and therefore did not transpose it in their national legislations, does not solve the problem that might occur if a patient would refuse to give his consent to the filling of a patent application for an invention made on the basis of biological material he gave.[51]

---

[49] The *spin-off* theory was developed in the Netherlands in the late 90's and as already been examined by the European Court of Justice which adopted it in the case *Fixtures Marketing Ltd v. Organismos pronostikon agonon podosfairou AE (OPAP),* ECJ, 9th November 2004, 444/02, Rec., p. I-10549.

[50] Directive 98/44/EC of the European Parliament and of the Council of 6 July 1998 on the protection of biotechnological inventions, *OJ* L 213, p. 13-21.

[51] For details on this matter see « Intellectual property on medical data - chimaeras and actuality », *opcit,* p. 753-755.

2.4.9. What about Intellectual Property Rights and healthgrids' Components?

The **Directive on the legal protection of computer programmes** [52] was a real European 'first' for copyright law. The first copyright measure to be adopted following the publication of the White Paper on completing the Single Market by 1992, the Directive aims to harmonise Member States' legislation regarding the protection of computer programmes in order to create a legal environment that affords a degree of security against unauthorised reproduction of such programmes.

In accordance with the Directive's provisions, the Member States are obliged to protect computer programs by copyright, as literary works within the meaning of the Berne Convention for the Protection of Literary and Artistic Works.[53]

The core principles of the Directive state that a computer program shall be protected if it is original in the sense that it is the author's own intellectual creation, the author of a computer program is the natural or legal person or group of natural persons who created it and where collective works are recognised by the legislation of a Member State, the person considered by the legislation of that Member State to have created the work is deemed to be its **author**[54] or may be owned jointly.[55] The exclusive rights of the author of a computer program include the right to perform or to authorise:

(a) the permanent or temporary reproduction of his computer program by any means and in any form, in part or in whole[56];

(b) the translation, adaptation, arrangement and other alteration of his computer program and the reproduction

[52] Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *OJ* L 122, 17 May 1991, p. 42–46.

[53] Directive 91/250/EC on the legal protection of computer programs, art. 1(1).

[54] Directive 91/250/EC on the legal protection of computer programs, art. 2(1).

[55] Directive 91/250/EC on the legal protection of computer programs, art. 2(2).

[56] Insofar as loading, displaying, running, transmission or storage of the computer program necessitate such reproduction, such acts shall be subject to authorisation by the copyright owner of the program.

of the results thereof without prejudice to the rights of the persons who alters the program;

(c) the distribution, including the rental, of his original computer program or of copies thereof.[57]

Special protection measures will be taken against a person committing any of the acts listed hereunder:

(a) any act of putting into circulation a copy of a computer program knowing, or having reason to believe, that it is an infringing/a counterfeiting copy;

(b) any possession for commercial purposes of a copy of a computer program knowing, or having reason to believe, that it is an infringing/ a counterfeiting copy;

(c) any act of putting into circulation or the possession for commercial purposes of any means with the intended purpose of facilitating the unauthorised removal or circumvention of any technical device which may have been applied to protect a computer program.

The term of **protection** is granted for the life of the author and for fifty years after his death or after the death of the last surviving author in the case of collective works. When the author is anonymous or has used a pseudonym or where national legislation has appointed a legal person as the author, the term of protection runs from the time the computer program is first lawfully made available to the public. Directive 93/98/EEC on harmonising the term of protection of copyright

[57] On this point, it is important to underline that the Directive 91/250/EC foresees that the first sale in the Community of a copy of a computer program by the right holder or with his consent shall exhaust the distribution right within the Community of that copy, with the exception of the right to control further rental or the program or copy thereof.

and certain related rights, extended the duration of copyright protection to **seventy years**.

A further piece of European legislation on copyright was adopted in 2001 with **Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society**[58]**,** which sought to adapt legislation on copyright and related rights to technological developments and particularly to the information society. The objective was to transpose at Community level the main international obligations deriving from two Treaties[59] concerning copyright and related rights, adopted in December 1996 in the framework of the World Intellectual Property Organisation (also named 'WIPO'), in particular concerning reproduction rights, the right of communication and distribution rights.

2.4.10.Conclusion

Looking at the EU legislation around Intellectual Property Law and its application to healthgrids we have seen that rules around protection of databases and computer programmes are poorly adapted to dealing with the open and shared nature that underlies the grid concept.

A Community-wide harmonisation of the national legislations available for the protection of copyright and certain related rights mainly took place through the legal framework of the Directive on the Legal Protection of Databases mentioned above, which allows a harmonised protection of copyright and related rights in all the EU Member States. In this sense, the harmonisation of the national legislation will favour the implementation of healthgrids as services that can circulate freely without any barriers throughout an un-fragmented market.

[58] European Parliament and Council Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, *OJ* L 167, 22 June 2001, p. 10-19.

[59] These two Treaties were the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty.

On the other hand, copyrights can constitute an impediment in the implementation of healthgrids, given that copyright law treats computer software as a copyrightable literary work, the same as a play or a novel. The copyright owner has the exclusive right to reproduce his work, prepare derivative works, distribute copies to the public, perform the work publicly and display the work publicly. Under these circumstances, any natural or legal person would have to pay to use computer programs while they constitute one of the most important compounds of healthgrids.

The open standards software approach could then be a solution to help the development and implementation of healthgrids. In the United States, the open source model (being a more open system than open standards) currently uses copyright and contract principles to retain control of the work and could thus encourage use without dedicating the work to the public domain.[60]

[60] See Dennis M. KENNEDY, "A primer on open source licensing legal issues: copyright, copyleft and copyfuture, *20 ST. LOUIS U. PUB. L. REV.,* 2001, 345, p. 359-360; David MCGOWAN, "Legal implications of open-source software", *U. ILL .L. REV.,* 2001, 241, p.242-243. More generally see Open Source Initiative, at http://www.opensource.org.

3. ETHICAL CONSIDERATIONS – AN OVERVIEW

This overview of medical and biomedical ethics is to give a baseline introduction to the field. This baseline of ethical considerations will then be applied to healthgrids in subsequent deliverables, and the links with legal, social and economic issues made.

3.1. INTRODUCTION

There are, of course, many approaches to medical ethics, ranging across religious, legal, philosophical and applied ethics, spanning many hundreds, if not thousands, of years of scholarly thought. One of the earliest statements on medical ethics - and certainly the most quoted - is the Hippocratic Oath. Named after the famous Greek physician Hippocrates, this oath was written as a guideline for the medical ethics for doctors. Although the exact words have changed over time, the general content is the same: an oath of respect to those who have developed the science of medicine, and a pledge of respect to the patients as well as the promise to treat them to the best of the one's ability. Although the Oath is now not generally sworn at graduation ceremonies anymore, but has been updated and incorporated in to modern texts such as the Declaration of Geneva and, in the United Kingdom, into the statement of the Duties of a Doctor as published by the General Medical Council.

The first formal code of medical ethics to be adopted by a professional organisation was written by English physician Thomas Percival (1740-1804) in 1794 and adapted and adopted by the American Medical Association in 1846. This code of ethics, which provided a gold standard for professional physicians, dictated the moral authority and independence of physicians in service to others and their responsibility towards the sick, as well as the physician's individual honour.

While there are many differences in the labels used in medical ethics across the approaches, most agree on some fundamental aspects of ethical medical practice: the respect for the patient

as an individual, including a respect for his or her privacy; the duty to treat all patients equally and fairly; and the duty not to harm patients, either medically or through an abuse of power.

One of the most well known and most frequently sited medical ethics textbooks is Beauchamp and Childress' *Principles of Biomedical Ethics* (Beauchamp, T and Childress L, 1979) first published in 1979 and now in its fifth edition (2001). In this book the authors set our four principle of ethical behaviour in medicine and biomedical science. In this section we will briefly explore those four key principles and consider the way in which the use of grid computing technology in health care might pose particular issues for those principles:

- Autonomy
- Beneficence
- Non-Malfeasance
- Justice

Beauchamp and Childress propose these four key principles as 'prima facie' principles, meaning that they are binding unless and until they conflict with another ethical principle. At such a point, the two or more principles have to be weighed against each other and the most ethically imperative one must be followed. While Beauchamp and Childress do not offer a formula for this weighing of competing values, it is this skill which is most called upon in daily practice.

3.2. RESPECT FOR AUTONOMY

Literally, autonomy means 'self rule', that is the ability to make our own decisions on the basis of conscious thought and consideration. A basic principle of ethical medical behaviour is a respect of such autonomy of the patient by the medical professional in so far as such respect is compatible with equal respect for the autonomy of all potentially affected. Raanon Gillon (Gillon, R. 1994), commenting on the application of

Beauchamp and Childress' four principles in the British Medical Journal states:

> *In health care respecting people's autonomy has many prima facie implications. It requires us to consult people and obtain their agreement before we do things to them - hence the obligation to obtain informed consent from patients before we do things to try to help them.*

Respect for autonomy is usually listed as the first principle of medical ethics because it is believed to be the corner stone of good practice. It will require even mundane administrative practice, such as keeping appointment times, since unless we respect such times we cannot respect the right other people have to organise their lives as they see fit.

It also requires good communication in order that patients have adequate information about any proposed intervention and also so that healthcare professionals can establish if the patient indeed wants that intervention. It may be argued also that respect for autonomy includes respecting when patients do not want a lot of information; some patients do not want to be told about a bad prognosis or to participate in deciding which of several treatments to have, preferring to leave this decision to their doctors. As Gillon argues, "respecting such attitudes shows just as much respect for a patient's autonomy as does giving patients information that they do want" (Gillon, R. 1994).

However, in daily medical practice a core aspect of the duty of respect for autonomy is the **duty of confidentiality**. It is argued that showing respect for a person's autonomy is respecting their **right to privacy**. Furthermore the promise to keep confidential issues revealed about why a particular choice is made is core to respecting that autonomy since an aspect of running our own "life depends on being able to rely on the promises made to us by others. Without such promises of confidentiality patients are also far less likely to divulge the often highly private and sensitive information that is needed for their optimal care; thus maintaining confidentiality not only

respects patients' autonomy but also increases the likelihood of doctors being able to help them" (Gillon, R. 1994).

3.3. BENEFICENCE AND NON-MALFEASANCE

We have noted that respect of autonomy is key to helping patients, which leads us to the second of the biomedical ethical principles: to do good and not to do harm. The duality of this principle seeks to balance the fact that, in seeking to help patients, doctors may inevitably risk harming them. The principle requires therefore that health care workers, who are committed to helping others, must consider the principles of beneficence and non-malfeasance together and aim at producing net benefit over harm.

As already noted the principle of beneficence must be balanced by the principle of autonomy: it is generally accepted that there is no obligation of beneficence to others, since we cannot treat someone, albeit for their own good, without consent (since that limits their autonomy) unless to do so severely limits the autonomy of another or indeed harms another.

In medical ethics the traditional 'story' used to illustrate this conundrum is the problem of treating the child of a Jehovah's Witness with blood products. If an adult Jehovah's Witness refuses treatment then it is generally accepted that he or she may continue to refuse treatment even if to do so would mean death, since a rational adult has a right to respect of his or her autonomy (in law imbedded in the requirement for consent to treatment) and thus the doctor would not be entitled to override the adult's refusal even if to do so would save his or her life.

In the case of a child, however, the situation is different. A child is not accorded the same respect for autonomy and while generally the consent of the adult responsible for a child is required to treat a child a refusal of such consent can be overridden if the child will be significantly harmed. As a result we have, in jurisdictions across the European Union, provision for the courts to make order to treat a child notwithstanding the

parent or guardian's refusal of consent. In such a case therefore beneficence/non-malfeasance overrides autonomy.

Thus we see that in both in philosophical ethics and in practical ethics we have established an ethical duty of respect for autonomy, which is balanced against the duty to do good - or at least to do no harm. The nature of the balance is determined by the power of the parties involved.

A further problem in medical care will arise, however, when individual care is balanced against public good – when the respect for one person's autonomy may lead to harm to another or harm to the fabric of our society. The balance of these competing ethical principles is often exercised through law, creating Public Health legislation which call for compulsory reporting and treatment of certain diseases (e.g., tuberculosis, cholera) even when to do so would breach a patient's confidentiality and right to refuse treatment.

3.4. JUSTICE

In the balance of individual rights and benefits against the rights of others and the public good, we embrace the ethical principle of justice. The obligation to produce net benefit, however, must also require us to define whose benefit and whose harms are likely to result from a proposed intervention, and to consider these benefits within the bigger picture of a fair and just resource allocation. This problem of moral scope is particularly important in medical research and population medicine.

No ethical model will, of course, be bale to solve those problems, their role is instead clarifying their existence and highlighting the need to find balance wherever possible among competing needs.

3.5. ETHICS IN EHEALTH

Despite the fact that information technology has been used in the delivery of healthcare for well over 20 years now and despite the fact that all Member States of the European Union have now adopted eHealth plans, remarkably little has been written about the ethics of using these technologies in healthcare. One of the most abiding works is still that of Rippen and Risk published in 2000, which led to the adoption of the Internet Health Coalition's eHealth Code of Ethics.

The eHealth Code of Ethics sets out eight principles:

- candour
- honesty
- quality
- informed consent
- privacy
- professionalism
- responsible partnering
- accountability

The code is targeted at the provision of information via the Internet, rather than the use of information technologies directly in the care of patients and in professional decision-making. The emphasis is thus on ensuring that the consumer of a health related website knows where and how information for the site was obtained, why it is provided and to ensure that those providing such information to patients are responsible in their choice of partners and are ultimately accountable to the consumer for the information available on the site. These concepts are reflected in nearly all statements of good health websites practice, including the Health on the Net Code (http://www.hon.ch/HONcode/) the European Commission's Communication on Quality Criteria for Health related Websites (COM(2002)667).

4. ECONOMIC ANALYSIS FOR HEALTHGRID PLANNING

4.1. INTRODUCTION

Legal and regulatory issues are only one side of the non-technological challenges to implementing healthgrid based solutions in Europe. If we are really to plan effectively to get the most out of this technology, we need a thorough understanding of the economic and social drivers that might impact on the uptake of healthgrids. In the following section we therefore look at the factors that a thorough healthgrid roadmap should take into account if it is to be effective in supporting further development and ultimately uptake of grid based computing in the health sector.

Economic theory and practice is essentially concerned with the optimal allocation of limited resources that have *alternative* uses[61]. **Resources** are goods and services, which represent means towards an end – ultimately the satisfaction of the needs and wants of human beings, citizens in our society. It is often thought that economic analysis focuses only on perfect market mechanisms, where needs or wants are articulated as demand for physical goods and services in complete markets with competing suppliers and where trade and pricing are closely related. This, however, is not the case. Much of modern economic theory focuses on so called **failures of the market**. These include cases of imperfect and incomplete information in the marketplace, externalities and public goods, markets where competition is restricted, and resource allocation by mechanisms other than trading in markets. These are all features of the healthcare sector, requiring us to look in detail at such aspects as stakeholder groupings, their goals and incentives, like the benefits flowing to them.

However, before setting out the basic economic analysis tools which may be used in assessing healthgrids we need to define some key terms. Accordingly we will begin by looking at the prime objectives of a healthcare system and the roles of key actors in such systems with respect to their interests in and impact on the potential uptake of healthgrids, and the main externalities affecting healthgrids.

[61] Dernburg TF, McDougall DM: Macroeconomics (3rd edition), New York: McGraw-Hill, 1968, p. 41

4.2. PRIME OBJECTIVES OF A HEALTHCARE SYSTEM

Although the Member States of the European Union have a variety of different approaches to health services organisation and regulation, all EU health systems aim to ensure healthcare provision that is "patient-centred and responsive to individual need"[62].

All the Member States also aim to making the systems financially sustainable, while simultaneously safeguarding the core values of healthcare:

- **Quality** is achieved through a range of measures. In particular, providing high quality healthcare is a function of continuous training of staff according to accepted standards, dissemination of good practices and innovative knowledge, as well as monitoring and good clinical governance.
- **Safety** refers to a systematic approach to ensuring patient safety, including the management of risk factors. This includes adequate training for health professionals and protection against misleading information about health and healthcare.
- **Care that is based on evidence and ethics** is essential for providing high-quality treatment and ensuring sustainability over the long term. A primary ethical challenge is to balance the needs of individual patients with the financial resources available to treat the whole population.
- **Involving the patient** includes transparency of healthcare status, treatment procedures, options, and choices, as well as active participation of the patient in making these choices.
- **Redress**: "Patients should have a right to redress if things go wrong. This includes having a transparent and fair complaints procedure, and clear information about liabilities and specific forms of redress determined by the health system in question (e.g. compensation)" .[63]
- **Privacy and confidentiality**, as protected by national legislation and international law.

[62] " Council Conclusions on Common values and principles in European Union Health Systems", Document (2006/C 146/01), Official Journal of the European Union on 22 June 2006, pp. 1 - 5

[63] ibid.

Grid technologies, by allowing for more comprehensive and faster creation, monitoring, and update of the medical content of prevention and health promotion schemes, are expected to play an important role in creating more efficient, patient-centred systems of healthcare that are able to sustain those core values. It is important therefore that in order to understand the potential of healthgrids and in order to adopt sensible roadmaps for research on grids and their implementation in the health sector that we understand the key legal, economic and socio-organisational issues that are to be addressed.

If health is defined according to the WHO as a "state of complete physical, mental and social well-being and not merely the absence of disease or infirmity"[64] it should be possible to derive directly or indirectly all of the following health system tasks and objectives from the overall objective of delivering health efficiently, and healthgrid applications can usefully be assessed against their contribution to each:

- to improve health outcomes;
- to protect patient safety;
- to cope with rising demand from ageing populations and increased expectations;
- to make healthcare access more egalitarian, ensure equality of access across social strata and at-risk groups, older people, regions of countries and the Union;
- to accelerate innovation: translation of new research-based knowledge into practice;
- to improve public health: disease control, surveillance and preventive measures;
- to protect the public against bio-terrorism and other new threats;
- to accelerate knowledge creation in research (medical, bio-medical, pharmaceutical, medico-technical, bio-informatics and ICT);
- to improve the quality of services;
- to reduce errors, duplicative and inappropriate care;

[64] Preamble to the Constitution of the World Health Organization as adopted by the International Health Conference, New York, 19-22 June, 1946; signed on 22 July 1946 by the representatives of 61 States (Official Records of the World Health Organization, no. 2, p. 100) and entered into force on 7 April 1948 (see: http://www.who.int/about/definition/en/

- to augment knowledge and capabilities of healthcare staff (continuous professional development);
- to improve quality of life perceived by patients;
- to improve quality assurance in hospitals and other health and social care providers;
- to manage citizen (patient) mobility and the free movement of professionals;
- to contain costs;
- to allocate resources optimally according to commonly agreed health policy priorities;
- to make best use of private service providers, international hospital chains, private equity, cross-border cooperation.

4.3. KEY ACTORS IN HEALTHCARE SYSTEMS

An essential part of any social and economic analysis of the potential impact of a new policy package is an assessment of the key stakeholder groups who could have an impact on acceptance of policy and implementation of new healthcare models. It is important therefore to identify who the key actors are, what their respective costs and benefits in the execution of any new policy package might be, and which facilitators and barriers may exist towards implementation and diffusion of new ICT-based solutions.

Based on a typology of actors and roles relevant in health system activities developed by the eHealth ERA project[65], the following is an illustrative list of possible actors and stakeholders in healthgrid applications:

- **Healthcare provider organisation**: an organisation, or part of such, engaging in healthcare activities. A self-employed doctor or other person is an organisation in this sense.
- **Healthcare professional**: an employee of a healthcare provider organisation.
- **Healthcare organisations** (organisations employing personnel providing specific healthcare services to patients): Health centres, hospitals, emergency services, imaging centres,

[65] www.ehealth-era.org

laboratories, pharmacies, doctor, dentist, midwife, nurse, chiropodist.

- **Public health bodies** (epidemiology data gatherers - for health information see healthcare information providers): European Commission, WHO, Ministries of health, local government.
- **Healthcare information and knowledge providers** (organisations and individuals authoring and/or publishing electronically or on paper information about healthcare and medical knowledge for citizens, patients and healthcare personnel): include universities and colleges, publishers, authors, editors, web-site providers; and research organisations.
- **Healthcare suppliers** (organisations trading in goods and services that enable provision of specific healthcare services but are not themselves specific healthcare services): include pharmaceutical companies, providers of medical equipment, ICT suppliers, and pharmacies.
- **Healthcare policy-makers**: ministries of health, local authorities, municipalities, World Health Organisation, European Institutions (e.g. European Commission DG Health and Consumer Protection).
- **Healthcare insurers** (bodies acting to insure and compensate for or reimburse costs for individual patients): include public health insurances, private health insurances, and national health services.
- **Doctors** include those individual roles in the provision of specific healthcare services usually requiring a medical doctorate including physicians, gynaecologists, surgeons, oncologists, anaesthetists, paediatricians, dentists, ...
- **Nurses**: individuals with nursing qualifications, whether working as community nurses, in doctors' surgeries or in hospitals.
- **Healthcare ancillary staff**: healthcare location managers and administrators, porters, cleaning staff, and others.
- **Other healthcare personnel**: midwives, paramedics...
- **Patients**: individual citizens having suffered an injury or attack of an illness and before that illness or injury is fully cured; or, more generally: citizens having suffered a health-threatening

event and before the impact of that event has been eliminated / has become irrelevant.

- **Citizens** not (yet) suffering, but being affected by environmental risks, health promotion, knowledge about diseases and their prevention, requiring information about health lifestyles …
- **Self-helping citizens**: Patients and other citizens operating in the role of healthcare personnel (determining medication, monitoring vital signs, monitoring for signs of illness…)
- **Informal carers**: private citizens not necessarily formally educated in healthcare providing specific healthcare services to one or more patients.
- **Insurances and other third party payers**, whether within a social insurance system or in a complementary private system.

This typology is designed as a typology of actors and roles rather than stakeholders, the economic/payer view is therefore perhaps underrepresented. We may need to add the roles of taxpayer and insurance premium payer among others. Though these roles may coincide with “patient” or “self-helping citizen” in the same individuals at any time, this is certainly not always the case, and any analysis should maintain these stake holdings as distinct.

In evaluating healthgrid applications, an appropriate values perspective is that of the social planner, taking all actors and stakeholders into account. At the same time attention should also be paid to how incentives can be provided to ensure investment actually goes ahead in cases where cost and benefit flows are to different stakeholder groups, and where the financial benefits that usually guide decision makers are not sufficient.

For the particular case of healthgrid technologies, an important issue in this respect is the fact that an organisation is providing its resources all the time, but only accessing resources for limited periods. With competition in the R&D sector, for example, where payoffs and risks are high, some organisations may not have an incentive to cooperate because of the further increased risk of a competitor being first in an invention who might, through the use of a

healthgrid system (for example in drug discovery) use resources of a 'loser' for his own gain.

4.4. IMPORTANT EXTERNALITIES IN ASSESSING HEALTHGRIDS

In economic analysis, **externalities** are defined as the impact of actor A's activities on actor B, who is not directly involved in that activity. Externalities are a particularly important feature of healthcare and a source of serious market failure[66]. For example, when a doctor invests in a new diagnosis support instrument, he probably takes into account the effects on his work, such as less time spent on diagnosis, and probably on the patient insofar as patients are more satisfied. However, the investment has a much larger impact – from the insurance company, which may see its expenditures reduced because illness is discovered at an earlier stage, to an increase in the total output of the economy due to the associated decrease in sickness leave. The problem faced by classical economic evaluation and assessment methods is that there is no market for, and thus no price, for an externality[67]. What is often referred to as broader effects on society and the economy[68] are, from an economic point of view, externalities in one form or another.

In a market setting it is usually the main beneficiary of a service who pays, and investments are only made if adequate returns accrue to the party making the investment. In healthcare, flows of benefits may diverge from flows of costs. In particular, studies show that patients can benefit extensively from eHealth applications, but healthcare providers are often the main entity financing eHealth investment[69]. "Private" benefits to providers may not provide sufficient incentive in respect of these investments, whose social benefits may nevertheless

---

[66] For a good introduction see Varian, H.R.: Intermediate Microeconomics: A Modern Approach, 6th ed., Norton, 2002

[67] This is the definition of externality. The most common examples of externalities are negative – like the environmental damage from a factory having an impact on a biological products farm. Here we are dealing mostly with positive externalities.

[68] For example in a recent report by the UK Evaluation Forum "Medical research: assessing the benefits to society" (2006),

[69] Jones T (2003) e-Health - Financial and Economic Case Studies, ACCA (The Association of Chartered Certified Accountants) with the European Commission DG INFSO, http://www.accaglobal.com/pdfs/members_pdfs/publications/m-eh-001.pdf

constitute a very substantial return to society as a whole. More recent evidence[70] shows two no less important issues:

- the benefits are often non-financial, which thwarts eHealth investments that should be made from an economical point of view;
- many potential investors, in particular healthcare provider organisations, do not realise what the scope of the benefits to themselves is.

4.5. A SIMPLE ECONOMIC AND SOCIAL ISSUES ANALYSIS OF HEALTHGRIDS

Having established the key stakeholders and primary objectives and externalities relevant to an understanding of healthgrids, we can now outline a simple economic analysis of the potential impact of healthgrids. Like in our assessment of the legal and regulatory aspects of healthgrids, the aim is to provide a baseline of common information against which a roadmap that highlights the bottlenecks and challenges to the implementation of healthgrids can be developed.

Socio-economic evaluations of healthgrid applications, as of other areas of eHealth, can help provide evidence-based information enabling them to identify appropriate targets for investment, and specifically to identify:

- type and scope of *benefits* for patients, carers, healthcare professionals, healthcare provider entities and other stakeholders in taking decisions to invest in eHealth applications;
- *de facto* beneficiaries and cost bearers of eHealth;
- number and type of *users*, their levels of utilisation, and so required and future capacity;
- impact on meeting *demand;*

[70] eHealth IMPACT: Study on the economic impact of eHealth, commissioned by the European Commission DG INFSO; http://www.ehealth-impact.org. For a summary report, see Karl A. Stroetmann, Tom Jones, Alexander Dobrev, Veli N. Stroetmann: eHealth is Worth it - The economic benefits of implemented eHealth solutions at ten European sites. Luxembourg: Office for Official Publications of the European Communities, 2006 (56 pp. - ISBN 92-79-02762-X). Electronic file: http://europa.eu.int/information_society/activities/health/docs/publications/ehealthimpactsept2006.pdf

- enabling *changes* that become possible to introduce new healthcare models and regional provider networks;
- benefits for clinical audit and governance;
- impact on established organisations, their structures, hierarchies, and workflows;
- scale of the critical investments needed in training and change management;
- potential changes to the costs of providing healthcare and the potential to generate additional income;
- impact on the future ICT infrastructure needed to support eHealth;
- impact on third party payers.

Evaluation can help remove inhibitors, show best practice, support future investment decisions and create enablers for change in eHealth. This is particularly important in Europe today, where eHealth is far from having become an integral part of routine medical service processes, beyond support for basic administrative processes or isolated applications in hospitals, medical labs and the like. In recent comprehensive empirical European market studies, it was shown that diffusion of advanced applications is still very limited or entirely lacking. The lack of reliable, transferable empirical evidence of eHealth effectiveness and outcomes, and of its cost and benefit efficiency, is widely seen to be a significant part of the problem.

However, even if fully reliable and validly transferable evidence shows a positive rate of return on investment (ROI) for eHealth, this will not be sufficient to convince many health system stakeholders. Besides reliable, easy to use technology and positive outcomes in medical and/or financial/economic terms, the policy and organisational aspects of the processes of implementation, change and diffusion can take on a more significant, and unfortunately often hindering aspect.

Organisational and systems views are important. Readiness, training, acceptance by all, win-win situations for all stakeholders, are some of the additional factors that will impact on the process of eHealth

implementation and diffusion.[71] These factors must be known in order to analyse the effect of using new technologies like healthgrids.

However, robust analyses of the effects of using new technologies are rare and nearly non-existent with respect to healthgrids[72]. Identifying the positive as well as negative impact of such new technologies and in particular the benefits from using them is critical to building an environment of well-informed decision making and successful implementation of beneficial technological solutions.

4.6. ECONOMIC ASSESSMENT MODELS / APPROACHES

There are a number of economic analysis techniques and metrics that are applicable to eHealth evaluation and analysis. The mainstream economic analysis techniques and models most relevant for eHealth applications evaluation are:

- Cost benefit analysis (CBA) (quantitative, monetary scale)
- Cost utility analysis (CUA) (qualitative scale)
- Cost effectiveness analysis (CEA) (achieving the best possible outcome for a given [fixed] cost)
- Cost minimisation analysis (CMA). (minimising the costs of achieving a fixed outcome)

[71] May C et al. (2003) Why do telemedicine systems fail to normalize as stable models of service delivery? Journal of Telemedicine and Telecare 9 (Suppl. 1):25-26

[72] The 'Joint White Paper from the healthgrid association and Cisco Systems' "HEALTHGRID – A SUMMARY", (http://whitepaper.healthgrid.org) for example states even that there are indeed very few "cases that demonstrate the benefits of dramatically new technologies (like GRID)". The economic analysis accompanying most of these few cases is very limited.

The following supporting techniques and measures are both used in the above types of analysis or may provide independent metrics for economic assessment:

- Marginal Net Present Value calculation (MNPV)
- Discounting (Present Value calculations)
- Payback period and breakeven point analysis
- Affordability gap analysis (AGA)
- Utilisation review (UR)
- Value chain analysis (VCA)
- eHealth utilisation (EHU) analysis
- Different approaches to costing
- Taking into account contingencies and risks.

Key methods and approaches are summarised as follows:

Cost benefit analysis is a measure of economic or monetary allocative efficiency. It identifies and measures the total costs and benefits of a project, which may include social costs and benefits, in monetary values. These are discounted to a net present value (NPV) to reflect the opportunity cost of time. The resulting discounted costs and benefits can be presented as a benefit/cost ratio, or as the value of net benefits (total net present value of benefits minus total net present value of costs). Where a number of options are being evaluated, these can be compared in order to identify the most profitable option. A key methodological issue is how to affix monetary values to individual and societal benefits.

Cost utility analysis is a measure of technical and allocative efficiency. It measures the cost of a particular treatment or type of care and compares it to the effects, expressed in additional utility to the patient. Utility can include anything from a subjective feeling of satisfaction to objective factors such as being alive and not suffering illness. Often, Quality Adjusted Life Years (QALY) are used as a unit of utility. Comparing the costs per additional QALY allows decision makes to identify the investment option that increases patient's utility the most, given the resources available.

Cost effectiveness analysis is a measure of *technical* efficiency. It identifies and measures the costs of different options for achieving a required outcome. Alternatively, this is the same as the option that delivers maximum output at a given cost. In contrast to a CBA, one part of the input/output ratio has to be fixed.

Cost minimisation analysis is a variant of cost effectiveness where all outcomes are set as equal. It identifies and measures the changes in unit costs to a healthcare provider that arise from a specific group of activities.

Discounting (Present Value calculation) is the technique by which monetary values from different points in time are converted into comparable measures. Usually, it is absolute monetary values in the future that are reduced in order to show their value at present – thus accounting for the opportunity cost of time (interest, utility from consumption now instead of later, risk, etc.). Discounting is particularly important in evaluating long-term investments where the benefits (returns) arise much after the point of investment expenditure. It also enables costs of projects with different life cycles to be compared.

Net present value identifies and measures the economic return to a commercial, private entity, from a specific investment in resources to achieve improved performance. It is discounted at the organisation's cost of capital to reflect the time value of money. It is a decision tool for the guidance of private investors who seek to rank projects in order of their profitability.

Payback period and breakeven point reveals the time that an entity has to wait to recover its investment in a project. It relies on the relationships between estimated cash flows going out of, and coming into a project. It disregards cash flows beyond the payback point. Its limitations as a measure are compensated by the need to ensure cash flows from a project are successful and that the inherent, increased risk of future cash flows are managed effectively. The payback period is the time span from the start of a project to its breakeven point (the point in time where cumulative income just covers cumulative costs). Breakeven analysis can also refer to a single time unit (like a year). In

that case it measures whether expenditure is covered by income within that particular year.

eHealth utilisation analysis identifies and measures the extent to which, and when, an eHealth investment is used over time. It can be applied at the point of care and at the link between healthcare professionals and their teams. It relies on data of transaction volumes for the eHealth application, and reflects acceptance, appropriateness and impact, and can be used to test the relative timing of eHealth cost and benefit curves.

Types of costing tool The main types are variable and fixed costing, total absorption costing, and activity based costing.

Types of cost: **Variable costs** vary directly with the numbers of patients. **Fixed costs** are commitment to expenditures that remain exactly the same for any volume of patients over the specified time horizon. There is also a classification of **semi-variable costs**. These change with stepped changes in volume, and can be the most important to identify. There are likely to be several semi-fixed costs for an eHealth application that covers several healthcare groupings. Variable costing can also be used to measure costs where eHealth results in a benefit that is in effect a change in costs. This could be fewer journeys by patients, making a benefit of the eHealth intervention, or a reduction in travel costs. Another example is where an eHealth application means that fewer pathology tests are carried out for a patient. The small reduction in costs e.g. of chemicals and reagents can be captured using variable costing. Where a change in the number of patients occur, say due to improved access, then the variable costs would change for a raft of resources, such as drugs, test consumables and medical supplies.

Activity based costing: Some years ago, the rigour of apportionment to types of cost was challenged[73] and the concept of activity based costing (ABC) introduced. ABC sought to improve the apportionments in total absorption costing by identifying and applying cost drivers. It also proposed that costing models should be extended beyond the

[73] Relevance Lost The Rise and Fall of Management Accounting. H Thomas Johnson, Robert S Kaplan, Harvard Business School Press, Boston Massachusetts 1987

entity so that knock-on cost changes could be included in the costing model. Our experience is that activity based costing concepts are valuable in the productivity evaluation of eHealth. However, its application tends to be costly and therefore in any specific decision setting the cost of improving information quality this way must be weighed against the possibly marginal value of increased decision certainty.

Contingencies in this setting are for correcting optimism bias and the impact of estimated risks on measurements and outcomes. Evaluations have a tendency to understate costs and overstate benefits. This increases where the basis of estimates relies more on judgement than facts and where the person making the judgement has an incentive to overestimate performance.[74]

4.7. APPLYING THE EHEALTH IMPACT METHODOLOGICAL FRAMEWORK TO HEALTHGRIDS

Clearly, when considering the wide variety of methodological approaches and options available, a choice has to be made. The review undertaken and our assessment of the usefulness of various methods identified led us to conclude to make use of the eHealth IMPACT[75] approach. It was developed as part of the eHealth IMPACT study which assessed ten successful, sustainable eHealth solutions across the full spectrum of potential application areas, and it is being used for evaluating further eHealth solutions. These range from an electronic health record system to nation-wide exchange of medical messages or supply chain management. The methodology needed for the eHealth IMPACT study was identified and developed from a focused review of state-of-the-art of economic evaluation techniques and assessments of ICT applications in healthcare and beyond. **CBA (Cost Benefit Analysis)** became the preferred economic concept. The intentionally generic nature, flexibility and adaptability of the methodology to specific instantiations of the wide variety of eHealth solutions allow the economic evaluation and assessment of the use of grid technologies in health services, including research.

---

74 HM Treasury, www.hm-treasury.gov.uk London, 2003

75 www.ehealth-impact.org

The eHealth solution to be assessed is approached from a socio-economic perspective, comprehensively identifying all relevant costs and all major benefits for all stakeholders: citizens/patients, healthcare provider organisations, and third party payers. The method focuses on measuring **net economic gains**: the difference between the economic values of direct benefits minus the identified costs; **eHealth utilisation**, defined as the usage of the service that is supported by ICT; and productivity. **Productivity** is measured by changes in the unit cost of the service provided. Economic variables are followed through three periods in the lifecycle of the eHealth application: planning and development, implementation, and routine operation. The method can be used both for ex-post evaluation and ex-ante assessment based on past experience and forecasts of future values.

Costs are divided into two main categories: **investment costs** and **costs of running** the healthcare related service. eHealth investment includes initial and replacement costs for ICT hardware and software, and costs of process and organisational change. Change management resources are a critical factor in benefits realisation. Operational costs include mainly staff costs, for professionals and support staff, and related other healthcare process costs. Costs are analysed by how they change as a result of the eHealth investment, both increases and reductions over time. Benefits are identified from the respective stakeholder groups involved. They cover three main categories: quality, access and efficiency. Quality includes the following subcategories: informed citizens, patients and carers; information designed around the citizen; timeliness of care; safety; and effectiveness.

For the concrete case of healthgrid applications, the following examples illustrate some intuitive benefit factors and potential methods of estimating their monetary value.

- **Time savings** from faster access to database search results, due to more computer power. The value of this can be calculated using the pay rate of staff doing the search. This would only apply to searches within databases accessible without the grid application.
- **Access** for professionals to larger, or joined, clinical and research **databases for clinical purposes**. The value can be estimated

using data on the frequency of access and change the clinical results due to the availability of this additional data.

To allow for an economic assessment, all benefits must be assigned a monetary value. Where no market prices, prices inferred from similar contexts or monetary values of time saved etc. are available, other estimations are required; these are always based on conservative assumptions. Willingness to pay (WTP), inferred from behaviour, is a common and accepted estimation method also used in eHealth IMPACT evaluations for the monetary value of intangible benefits that have no market price. All monetary values are converted into comparable measures by presenting them in present values.

The extensive use of estimated values, indispensable for a pragmatic approach to measuring the past, and particularly the future impact of eHealth, requires adjustments for optimism bias and contingencies. The size of the adjustment depends on the availability and quality of the actual estimates. A sensitivity analysis further helps test and verify the results for possible weakness of the available data.

The eHealth IMPACT methodology was tested and refined on ex-post evaluations, due to pragmatic reasons of data availability. However, the design allows equally for ex-ante assessments of the impact of investing in ICT in health services, the risks involved, and identification of key success factors. Given the limitation of funds available to health systems, such assessment is critical for achieving optimal allocation of resources.

The experience and results from the 10 evaluations undertaken as part of the eHealth IMPACT study, and the preliminary indications from two extra studies, can be taken forward to a business case for investment in eHealth. Of course, additional aspects, like financial analysis, affordability, and risk have to be taken into account, yet the generic economic case for future eHealth investment can be constructed using the knowledge from eHealth IMPACT. In the concrete case of healthgrid in health services and research, this would, however, be a highly complex and time consuming task.

5. GENERAL CONCLUSION - HIGHLIGHTING THE POTENTIAL LEGAL AND ECONOMIC BOTTLENECKS FOR HEALTHGRIDS IN EUROPE

The preceding pages have set out in some detail the existing EU level legal tools as well as economic principles which are important in understanding the potential bottlenecks for healthgrids in Europe.

In the section on legal issues, we looked at legislation concerning Data Protection, Liability for Goods and Services and Intellectual Property Rights. In the section on economic issues, we considered wider social values of health and health systems and the key actors with social and economic interests in such systems. We then considered the common economic tools used to assess the economic value in health and in particular in eHealth -we ended by looking at the value assessment model proposed in the eHealth IMPACT study.

Looking back at the discussion on Data Protection we can see that in broad terms the current EU level legislation is adequate but not ideal for promoting healthgrids. The discussion of the basic concepts and duties of the Data Protection Directive and its impact on healthgrids shows that, when healthgrids are used for treating patients or planning care, the requirements of the legislation provide that the data are collected and processed by medical professionals and the balance of rights weighs in favour of data collection – that is, it is assumed that the patient’s general interest in obtaining treatment or advancing medical care outweighs his interests in privacy.

The current legislation is not, however, adequate to support most of the longer running research initiatives around which healthgrids are based. As the current EU level legislation stands, Member States can enact specific legislation covering specific tools such as healthgrids in order to exempt scientists and medical practitioners using healthgrids from some of the more onerous duties of the Directive.

Member States could, for example adopt specific legislation to encourage the linking of diagnosis specific databases across a region or state in order to support research into a given disease. However, to

date, no Member State has addressed legislation to this particular issue and so healthgrids drawing the data and data processing power of many hospitals are burdened with onerous data protection requirements which could deter scientists from using adopting healthgrid technology and using its enhanced computational and data acquisition power.

The examination of the EU level legislation on Liability for Goods and Services shows that it is not at all adapted to the healthgrid domain. One of the reasons for this is, of course, that health services are organised at national or regional level and that the European Union has no legal competence to draw up legislation that states specifically how a health service should be organised.[76]

However, the EU does have a range of legislation designed to protect citizens from harm resulting from goods offered on the market. Steps could be taken using guidelines, or even specific legislation, to address distributed computing services, such as healthgrids, which would seem at present to be only marginally covered by the existing rules. Accordingly it is important that the existing European framework of general product safety is re examined to consider its applicability to distributed networks such as healthgrids.

Furthermore, the law on medical devices is very unclear with respect to healthgrids: while it may be argued that a healthgrid could fall within the ambit of the current Medical Devices Directive in that it is a software tool that impacts on a medical act, the whole construction of the Directive is based upon physical goods (which might have a software component) placed on the market for purchase or lease. It is thus ill adapted to deal with the shared domain of grid-based services where software sold and owned by a wide range of participants in a grid initiative.

It would seem therefore that at present the only real way to have clarity over liability for possible negative effects of healthgrids is through tightly constructed contracts in private law. If however the use of healthgrids across EU and international borders in shared

[76] Treaty of the European Union Art. 152 provides that matters of health services organisation are subject to the rule of subsidiarity and limits the role of the EU to support and co-ordination.

public/private initiative is to become a reality then steps should be taken to develop guidelines and possibly legislation to harmonise the legal expectation of all actors in a healthgrid. As an interim step to EU legislation in this area, it could be suggested that a suitable body, such as the High Level Group on Healthcare, is established.

However, to move healthgrids beyond the domain of university led and funded research tools we would need to address squarely the need to develop robust tools for sharing of the intellectual property inherent in the design and population of a healthgrid application.

As the law currently stands, the rules of copyright are very protective and could constitute an impediment in the implementation of healthgrids because they treat computer software as a copyrightable literary work, the same as a play or a novel.

The owner of the copyrighted software running a healthgrid has the exclusive rights to reproduce his work, prepare derivative works, distribute copies to the public, perform the work publicly and display the work publicly. Under these circumstances, any natural or legal person would have to pay to use computer programs while they constitute one of the most important compounds of healthgrids. Given that most Grid applications will depend on shared access to multiply copyrighted programmes it is unlikely that such a model of copyright is useful in protecting the entirety of a healthgrid application.

An open standard approach to software co-development could help the development and implementation of healthgrids. The open source licensing model actually uses copyright and contract principles to retain control of the work while enabling its use effectively for free and could thus encourage use and development.

All such legal fine-tuning, whether through standardised contracts, special data sharing agreements or open standards based software development will be of little use in driving forward the development and implementation of healthgrids if the social and economic settings are not examined thoroughly in order to develop fully weighed up

cost-benefit and cost-utility based assessments of the use of healthgrids in healthcare delivery.

Reflecting on the Socio-Economics Section, it becomes obvious that the uptake of healthgrid systems and solutions will also heavily depend on the extent to which they can help address problems and challenges of health systems. Such impact is presumed, yet there is little evidence of its scope. Detailed analysis of existing applications, as well as ex-ante assessments of the benefits from the future use of healthgrids will prove essential for mobilising the required will and enthusiasm among research funding entities, political organisations and society at large. Potential benefits include time savings, particularly important in cases of potential pandemics, and access to better quality clinical and research data leading to improvements in the quality of clinical outcomes. The methodological framework developed and described above renders an adequate methodological framework for providing evidence on these benefits.

The same framework can also be used as the basis for addressing another inhibitor to a widespread adoption of healthgrid solutions – lack of (knowledge about) private incentives. A business case for the routine use of grid technologies in the health sector is essential for moving from project-based, exemplary utilisation to a widespread uptake of healthgrid-based solutions.

We expect that the evaluation of currently running, exemplary healthgrid solutions will aid the design of the right incentives for particular stakeholders, which, facilitated by the appropriate legal framework, will ensure the wider adoption and uptake of healthgrid.